Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On the Quaternary Linear Homogeneous Group and the Ternary Linear Fractional Group.

By T. M. Putnam.

§1.—Introduction.

The general group of linear homogeneous substitutions on m indices, with coefficients arbitrary marks of a Galois field such that the determinant is unity, contains an invariant subgroup made up of all those substitutions that multiply every index by an m^{th} root of unity in the field. If $d = [m, p^n - 1]$, then the equation $X^m = 1$ has just d solutions in the field in which we are working,—the $GF[p^n]$, so that this invariant subgroup is of order d.

It has been shown[*] that the quotient-group defined by this invariant subgroup is simple, and is holoedrically isomorphic with the linear fractional group on $m - 1$ indices. The order of the general homogeneous group of substitutions with determinant unity is

$$M = (p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{2n}) \cdots\cdots (p^{nm} - p^{n(m-1)})/(p^n - 1).$$

Hence, the linear fractional group is of order $N = \frac{1}{d} M$.

In a previous paper[†] the writer has studied the distribution of the substitutions of the homogeneous group into complete sets of conjugate substitutions for the case $m = 4$, and for arbitrary determinant. It is proposed here to consider the same properties when the determinant is unity, both for the homogeneous group and for the fractional group on three indices. The periods of all the substitutions in both groups will be determined and, as far as possible, the arrangement of the cyclic subgroups into conjugate sets will be investigated.* Certain commutative subgroups will occur in the investigation which will be studied in their abstract form (cf. §22).

---

[*] Dickson, Annals of Mathematics, vol. XI, pp. 161–183. Burnside, "Theory of Groups," p. 340.

[†] Amer. Journ. of Math., vol. XXIII, pp. 41–48.

The linear fractional group is further important in that according as p^n is of the form 2^n, $4l-1$, $4l+1$, it is simply isomorphic respectively, with the senary linear groups $FH(6, 2^n)$, $NS(6, p^n)$, $O(6, p^n)$, each defined by a quadratic invariant (Dickson, Bul. A. M. S., 1898–9, p. 472).

§2.—In this case $d = [4, p^n - 1]$, so that

$$d = 1, \text{ if } p^n = 2^n;\ d = 2, \text{ if } p^n = 4l - 1;\ d = 4, \text{ if } p^n = 4l + 1.$$

Since there are just d solutions of the equation $X^4 = 1$ in the $GF[p^n]$, there are d homogeneous substitutions of determinant unity,

$$\xi_i' = \theta^r(\alpha_{i1}\xi_1 + \alpha_{i2}\xi_2 + \alpha_{i3}\xi_3 + \alpha_{i4}\xi_4), \qquad [i = 1, 2, 3, 4],$$

which, when taken fractionally, lead to the same non-homogeneous substitution of determinant unity, θ^r running through the d roots of the equation $X^4 = 1$.

When $d = 1$, therefore, the linear fractional group G is holoedrically isomorphic with the homogeneous group H. When $d = 4$, we may derive the results for the group G by considering, as identical in H, the substitutions

$$S,\ \Theta S,\ \Theta^2 S,\ \Theta^3 S,$$

where Θ is the substitution multiplying every index by a primitive root θ of the equation $X^4 = 1$ (cf. §11). When $d = 2$, θ and θ^3 are not present in the field, and we may obtain the results for G in this case by regarding S and $\Theta^2 S$ as identical in H.

The discussion falls naturally, then, into the three cases $d = 1$, $d = 2$ and $d = 4$, which will be considered, as far as possible, together, though this will be impracticable in certain cases.

The foundation of the developments here presented rests on the theorem of Jordan,† on the reduction of homogeneous substitutions S on m variables to canonical forms, by transformation of indices, and more directly on its generalization to the $GF[p^n]$ by Professor Dickson.‡ The latter in his paper also sets up the corresponding simultaneous canonical form of a substitution commutative with S, of which theorem constant use will also be made.

---

* The corresponding properties for the case $n = 3$ has been carried out by Professor Dickson, Amer. Journ. of Math., vol. XXII, pp. 231–252.

† "Traité des Substitutions," pp. 114–126.

‡ Amer. Journ. of Math., vol. XXII, pp. 121-137.

§3.—If S is the substitution,

$$\begin{aligned} x' &= \alpha_{11}x + \alpha_{12}y + \alpha_{13}z + \alpha_{14}w, \\ y' &= \alpha_{21}x + \alpha_{22}y + \alpha_{23}z + \alpha_{24}w, \\ z' &= \alpha_{31}x + \alpha_{32}y + \alpha_{33}z + \alpha_{34}w, \\ w' &= \alpha_{41}x + \alpha_{42}y + \alpha_{43}z + \alpha_{44}w, \end{aligned}$$

then its characteristic equation $\Delta(\lambda) = 0$ is defined as follows:

$$\Delta(\lambda) \equiv \begin{vmatrix} \alpha_{11} - \lambda & \alpha_{12} & \alpha_{13} & \alpha_{14} \\ \alpha_{12} & \alpha_{22} - \lambda & \alpha_{23} & \alpha_{24} \\ \alpha_{13} & \alpha_{23} & \alpha_{33} - \lambda & \alpha_{34} \\ \alpha_{14} & \alpha_{24} & \alpha_{34} & \alpha_{44} - \lambda \end{vmatrix} \equiv \lambda^4 + a\lambda^3 + b\lambda^2 + c\lambda + 1 = 0,$$

where a, b, c are obviously marks of the $GF[p^n]$.

The substitution

$$x' = \alpha x - \beta y + \gamma z - w, \quad y' = x, \quad z' = y, \quad w' = z$$

has for its characteristic equation

$$\lambda^4 - \alpha\lambda^3 + \beta\lambda^2 - \gamma\lambda + 1 = 0,$$

where α, β, γ are arbitrary marks of the field. Hence they may be so chosen that $\Delta(\lambda)$ is irreducible; the product of a linear factor and an irreducible cubic; the product of two irreducible quadratic factors, distinct or equal; the product of an irreducible quadratic and two linear factors, distinct or equal; or, finally, the product of four linear factors, distinct, or some or all of them equal.

§4.—Following the general theorem cited in §2, we proceed to the enumeration of the canonical forms that will arise. The classification depends on the ways that $\Delta(\lambda)$ breaks up into factors in the field, and the results of §3 show that all possible factorizations will occur, though the equality of the factors will not be possible for certain low values of p^n.

Type 1. When $\Delta(\lambda) = 0$ is irreducible, its roots are of the form λ, λ^{p^n}, $\lambda^{p^{2n}}$, $\lambda^{p^{3n}}$, their product being unity, and λ belonging to the $GF[p^{4n}]$. The corresponding canonical form is

$$x' = \lambda x, \; y' = \lambda^{p^n} y, \; z' = \lambda^{p^{2n}} z, \; w' = \lambda^{p^{3n}} w, \qquad (\lambda^{p^{3n}+p^{2n}+p^n+1} = 1).$$

Type 2. If $\Delta(\lambda)$ has a cubic irreducible factor, the canonical form becomes

$$x' = \lambda x, \quad y' = \lambda^{p^n} y, \quad z' = \lambda^{p^{2n}} z, \quad w' = \lambda^{-(p^{2n}+p^n+1)} w,$$

where λ, λ^{p^n}, $\lambda^{p^{2n}}$ are the roots of the irreducible cubic factor equated to zero, and x, y, z are conjugate with respect to the $GF[p^n]$.

Type 3. If the equation $\Delta(\lambda) = 0$ breaks up into two distinct irreducible quadratic equations, whose roots are λ, λ^{p^n} and μ, μ^{p^n} respectively, the canonical form becomes

$$x' = \lambda x, \quad y' = \lambda^{p^n} y, \quad z' = \mu z, \quad w' = \mu^{p^n} w, \qquad [(\lambda\mu)^{p^n+1} = 1],$$

where $\lambda \neq \mu$ and $\lambda \neq \mu^{p^n}$, x and y, z and w being conjugates.

Type 4. For this case $\Delta(\lambda) = 0$ is the square of an irreducible quadratic with roots λ, λ^{p^n}. Two types of canonical forms will occur, viz.

$$\left.\begin{array}{llll} 4\,(\mathrm{i})\;\; x' = \lambda x, & y' = \lambda(y + x), & z' = \lambda^{p^n} z, & w' = \lambda^{p^n}(w + z), \\ 4\,(\mathrm{ii})\;\; x' = \lambda x, & y' = \lambda y \qquad , & z' = \lambda^{p^n} z, & w' = \lambda^{p^n} w \qquad , \end{array}\right. [\lambda^{2(p^n+1)} = 1].$$

Type 5. When $\Delta(\lambda)$ is the product of an irreducible quadratic factor and two distinct linear factors, the roots then being λ, λ^{p^n}, α, β, where α and β are in the $GF[p^n]$, the canonical form is

$$x' = \alpha x, \quad y' = \beta y, \quad z' = \lambda z, \quad w' = \lambda^{p} w, \qquad (\alpha\beta\lambda^{p^n+1} = 1, \alpha \neq \beta).$$

Type 6. If the linear factors in type 5 are equal, i. e. $\alpha = \beta$, two sub-types occur.

$$\left.\begin{array}{llll} 6\,(\mathrm{i})\;\; x' = \alpha x, & y' = \alpha y \qquad , & z' = \lambda z, & w' = \lambda^{p^n} w, \\ 6\,(\mathrm{ii})\;\; x' = \alpha x, & y' = \alpha(y + x), & z' = \lambda z, & w' = \lambda^{p^n} w, \end{array}\right. (\alpha^2\lambda^{p^n+1} = 1).$$

For all the remaining types, the roots of $\Delta(\lambda) = 0$ are in the $GF[p^n]$, the classification being based on the question of their being equal or distinct.

Type 7. If the roots are all distinct the form is

$$x' = \alpha x, \quad y' = \beta y, \quad z' = \gamma z, \quad w' = \delta w, \qquad (\alpha\beta\gamma\delta = 1).$$

Type 8. If two roots are equal, there are two forms,

$$\left.\begin{array}{llll} 8\,(\mathrm{i})\;\; x' = \alpha x, & y' = \alpha y \qquad , & z' = \beta z, & w' = \gamma w, \\ 8\,(\mathrm{ii})\;\; x' = \alpha x, & y' = \alpha(y + x), & z' = \beta z, & w' = \gamma w, \end{array}\right. (\alpha^2\beta\gamma = 1).$$

Type 9. When three roots are equal, we have the three forms,

$$\left.\begin{array}{llll} 9\,(\mathrm{i})\;\; x' = \alpha x, & y' = \alpha(y + x), & z' = \alpha(z + y), & w' = \beta w, \\ 9\,(\mathrm{ii})\;\; x' = \alpha x, & y' = \alpha(y + x), & z' = \alpha z \qquad , & w' = \beta w, \\ 9\,(\mathrm{iii})\;\; x' = \alpha x, & y' = \alpha y \qquad , & z' = \alpha z \qquad , & w' = \beta w, \end{array}\right. (\alpha^3\beta = 1).$$

Type 10. If all four roots are equal, five cases arise.

$$\begin{array}{lllll}
10\,(\text{i}) & x' = \alpha x, & y' = \alpha(y+x), & z' = \alpha(z+y), & w' = \alpha(w+z), \\
10\,(\text{ii}) & x' = \alpha x, & y' = \alpha(y+x), & z' = \alpha(z+y), & w' = \alpha w \quad , \\
10\,(\text{iii}) & x' = \alpha x, & y' = \alpha(y+x), & z' = \alpha z \quad , & w' = \alpha w \quad , \qquad (\alpha^4 = 1), \\
10\,(\text{iv}) & x' = \alpha x, & y' = \alpha(y+x), & z' = \alpha z \quad , & w' = \alpha(w+z), \\
10\,(\text{v}) & x' = \alpha x, & y' = \alpha y \quad , & z' = \alpha z \quad , & w' = \alpha w \quad ,
\end{array}$$

Type 11. If the roots are equal in pairs, there are three cases.

$$\begin{array}{lllll}
11\,(\text{i}) & x' = \alpha x, & y' = \alpha y \quad , & z' = \beta z, & w' = \beta w \quad , \\
11\,(\text{ii}) & x' = \alpha x, & y' = \alpha(y+x), & z' = \beta z, & w' = \beta(w+z), \qquad (\alpha^2\beta^2 = 1). \\
11\,(\text{iii}) & x' = \alpha x, & y' = \alpha y \quad , & z' = \beta z, & w' = \beta(w+z).
\end{array}$$

§5.—The above list of canonical forms is complete for the group of substitutions of arbitrary determinant. Furthermore, it is known* that if S and S' are any two substitutions reducible to the same canonical form, there exists a substitution W such that $S' = W^{-1}SW$; i. e. all substitutions reducible to the same canonical form are conjugate within the general group. The converse is also true.

For the group H of substitutions of determinant unity, it is necessary that two substitutions, having the same canonical form, shall be conjugate by means of a substitution of determinant unity. If the determinant of W be ω, and there exists a substitution T of arbitrary determinant τ such that $S = T^{-1}ST$, then choosing $\tau = \omega^{-1}$, the substitution TW will be of determinant unity and is such that

$$(TW)^{-1}S(TW) = S'.$$

It will be shown that the substitution T exists for all types excepting 4 (i), 10 (i), 10 (iv) and 11 (ii). The necessary subtypes will then be set up for these cases.

§6.—The substitution

$$x' = \alpha x, \quad y' = y, \quad z' = z, \quad w' = w$$

is commutative with substitutions of the canonical forms (5), 6 (i), (7), 8 (i),

---

* Dickson, Amer. Journ. of Math., vol. XXII, p. 136.

11 (i) and 11 (iii), and being of arbitrary determinant, may be taken as the T of the preceding articles for these types.

For type (1), T may be taken as

$$x' = \sigma^r x, \quad y' = \sigma^{rp^n} y, \quad z' = \sigma^{rp^{2n}} z, \quad w' = \sigma^{rp^{3n}} w,$$

where σ is a primitive root of the $GF[p^{4n}]$. Its determinant is $\sigma^{r(p^{3n}+p^{2n}+p^n+1)}$, but since the $(p^{3n}+p^{2n}+p^n+1)$th power of σ is a primitive root of the $GF[p^n]$, this determinant is equal to an arbitrary mark of that field.

The substitution

$$x' = x, \quad y' = y, \quad z' = z, \quad w' = aw$$

is commutative with one of types (2), 8 (ii), 9, 10 (ii) and 10 (iii), and is of arbitrary determinant; hence, may be taken as T.

For types (3) and 6 (ii), we may choose as T the substitution

$$x' = x, \quad y' = y, \quad z' = \sigma^r z, \quad w' = \sigma^{rp^n} w,$$

where σ is a primitive root of the $GF[p^{2n}]$. Since σ^{p^n+1} is a primitive root of the $GF[p^n]$, the determinant $\sigma^{r(p^n+1)}$ of this substitution is arbitrary in the $GF[p^n]$.

The most general substitution commutative with a substitution of type 4 (i) has the canonical form

$$x' = \sigma^r x, \quad y' = \sigma^r y + \sigma^s x, \quad z' = \sigma^{rp^n} z, \quad w' = \sigma^{rp^n} w + \sigma^{sp^n} z,$$

where the determinant is $\sigma^{2r(p^n+1)}$, σ being a primitive root of the $GF[p^{2n}]$. Putting $\rho = \sigma^{p^n+1}$, the determinant becomes ρ^{2r}. When $d = 1$, every mark of the $GF[p^n]$ is a square, hence equal to ρ^{2r} for a proper choice of r. When $d = 2$ or 4, only half the marks are squares, so that when ω^{-1} is a not-square, ρ^{2r} cannot be made equal to it. Since the product of a square and a not-square is again a not-square, we may choose r such that $\rho^{2r}\omega^{-1}$ is any particutar not-square t. Hence, any two substitutions S and S' reducible to the canonical form 4 (i), are conjugate by means of a substitution of the field of determinant 1 or t. Hence, for the group of determinant unity two distinct canonical forms arise for this type when $d = 2$ or 4. They may be chosen to be

$$\begin{array}{lllll} 4\,(\mathrm{i}) & x' = \lambda x, & y' = \lambda(y + x)\;, & z' = \lambda^{p^n} z, & w' = \lambda^{p^n}(w + z)\;, \\ 4'\,(\mathrm{i}) & x' = \lambda x, & y' = \lambda(y + \sigma x), & z' = \lambda^{p^n} z, & w' = \lambda^{p^n}(w + \sigma^{p^n} z), \end{array}$$

where σ is a primitive root of the $GF\,[p^{2n}]$. These are not conjugate by means of a substitution of determinant unity. For, the most general substitution transforming $4'\,(1)$ into $4\,(\mathrm{i})$ has the form

$$x' = a\sigma x, \quad y' = a\sigma x + ay, \quad z' = b\sigma^{p^n}z, \quad w' = c\sigma^{p^n}z + bw,$$

where x and z, w and y are conjugates respectively. The determinant of this substitution is seen to be

$$a^2b^2\sigma^{p^n+1} = a^2b^2\rho\,;$$

hence, it can never be equal to unity, and, therefore, for the group H, these forms are distinct.

The substitution

$$x' = \sigma^r x, \quad y' = y, \quad z' = \sigma^{rp^n}z, \quad w' = w$$

is commutative with a substitution of type $4\,(\mathrm{ii})$ and its determinant $\sigma^{r(p^n+1)}$, being arbitrary in the $GF\,[p^n]$, it may be chosen as T for this type.

The most general substitution transforming $10\,(\mathrm{i})$ into itself is

$$x' = ax, \quad y' = bx + ay, \quad z' = cx + by + az, \quad w' = ex + cy + bz + aw,$$

with determinant a^4. If $d = 1$, every mark in the $GF\,[p^n]$ is a fourth power, so that an a can be found such that $a^4 = \omega^{-1}$. When $d = 2$, $p^n = 4l - 1$. Hence $\rho^{4lk} = \rho^{2k}$, so that squares are also fourth powers. If ω^{-1} is a not-fourth power, then the equation $a^4 = \omega^{-1}.t$ can be satisfied, where t is any particular not-square. Hence, it follows, as for type $4\,(\mathrm{i})$, that when $d = 2$, two substitutions of this canonical form are conjugate by means of a substitution of determinant unity or t. Two subcases then arise which may be taken to be

$$\begin{array}{lllll} 10\,(\mathrm{i}) & x' = \alpha x, & y' = \alpha\,(y + x)\;, & z' = (z + y), & w' = \alpha\,(w + z), \\ 10'\,(\mathrm{i}) & x' = \alpha x, & y' = \alpha\,(y + tx)\;, & z' = (z + y), & w' = \alpha\,(w + z). \end{array}$$

When $d = 4$, then $p^n = 4l + 1$, so that squares are not always fourth powers as for $d = 2$. If ω is a not-fourth power, then $a^4\omega$ can be made equal to either t, t^2 or t^3, where t is a particular not-square. For, suppose $t = \rho^{4k+1}$, then $t^3 = \rho^{4k'+3}$. Hence, if $\omega = \rho^{4r+1}$, $t\omega^{-1}$ will be a fourth power, hence $a^4 = t\omega^{-1}$ can be satisfied, or $a^4\omega = t$. If $\omega = \rho^{4r+3}$, then $t^3\omega^{-1}$ is a fourth power, while if $\omega = \rho^{2h}$, then $t^2\omega^{-1}$ is a fourth power. Thus when $d = 4$, two substitutions reducible to this canonical form will be conjugate by means of a substitution of determinant 1, t, t^2 or t^3. In addition to types 10 (i) and 10$'$ (i), there will be two other subcases,

$$10''\,(\mathrm{i})\quad x'=\alpha x,\quad y'=\alpha(y+t^2x),\quad z'=\alpha(z+y),\quad w'=\alpha(w+z),$$
$$10'''\,(\mathrm{ii})\quad x'=\alpha x,\quad y'=\alpha(y+t^3x),\quad z'=\alpha(z+y),\quad w'=\alpha(w+z).$$

These four subtypes are indeed all distinct, for the most general substitution transforming

$$x'=\alpha x,\quad y'=\alpha(y+t^rx),\quad z'=\alpha(z+y),\quad w'=\alpha(w+z)$$

into the substitution

$$x'=\alpha x,\quad y'=\alpha(y+t^sx),\quad z'=\alpha(z+y),\quad w'=\alpha(w+z)$$

is the substitution

$$x'=a_1x,\quad y'=a_2x+a_1t^{s-r}x,\quad z'=a_3x+a_2t^{-r}y+a_1t^{s-r}z,$$
$$w'=a_4x+a_3t^{-r}y+a_2t^{-r}z+a_1t^{s-r}w,$$

with determinant $a_1^4t^{3(s-r)}$, which can never be unity for $s,\ r=0,\ 1,\ 2,\ 3,\ s\neq r$.

The most general substitution transforming type 10 (iv) into itself has a determinant a^2. By a discussion analogous to that used for type 4 (i), we find that when $d=2$ or 4, two subtypes are necessary which may be taken to be

$$10\,(\mathrm{iv})\quad x'=\alpha x,\quad y'=\alpha(y+x),\quad z'=\alpha z,\quad w'=\alpha(w+z),$$
$$10'\,(\mathrm{iv})\quad x'=\alpha x,\quad y'=\alpha(y+tx),\quad z'=\alpha z,\quad w'=\alpha(w+z),$$

where t is a particular not-square. These are not conjugate by means of a substitution of determinant unity.

The same state of affairs exists for type 11 (ii), the necessary subtypes being

$$11\,(\mathrm{ii})\quad x'=\alpha x,\quad y'=\alpha(y+x),\quad z'=\beta z,\quad w'=\beta(w+z),$$
$$11'\,(\mathrm{ii})\quad x'=\alpha x,\quad y'=\alpha(y+tx),\quad z'=\beta z,\quad w'=\beta(w+z),$$

where again t is a particular not-square.

§7.—In studying the particular canonical forms, the typical substitution will be denoted by S, and will be thought of as any substitution reducible to the canonical form, or as the canonical form itself. T will designate a substitution commutative with S, while M will denote the order of the homogeneous group H, viz.

$$M=(p^{4n}-1)(p^{4n}-p^n)(p^{4n}-p^{2n})(p^{4n}-p^{3n})/(p^n-1),$$

and N will stand for the order of the fractional group G, where $N=\frac{1}{d}M$.

Type 1.

§8.—Among the substitutions of this type occurs

$$S\colon\quad x' = \lambda x, \quad y' = \lambda^{p^n} y, \quad z' = \lambda^{p^{2n}} z, \quad w' = \lambda^{p^{3n}} w$$

such that λ is a primitive root of the equation

$$\lambda^{p^{3n}+p^{2n}+p^n+1} = 1.$$

Indeed, by §3, there exists a substitution whose characteristic equation

$$\Delta(\lambda) = \lambda^4 - \alpha\lambda^3 + \beta\lambda^2 - \gamma\lambda + 1 = 0$$

has its coefficients arbitrary marks of the $GF[p^n]$.

Any other substitution of this type will have as multipliers λ^r, λ^{rp^n}, $\lambda^{rp_2{}^n}$, $\lambda^{rp^{3n}}$, and is, therefore, a power of S. The period of S is $p^{3n} + p^{2n} + p^n + 1$ while that of the corresponding substitution in G is the least integer m such that

$$\lambda^m = \lambda^{mp^n} = \lambda^{mp^{2n}} = \lambda^{mp^{3n}}.$$

Hence $m(p^n - 1)$ is a multiple of $p^{3n} + p^{2n} + p^n + 1$. But

$$[p^n - 1, p^{3n} + p^{2n} + p^n + 1] = [p^n - 1, 4] = d,$$

so that the period of S in G becomes

$$\frac{1}{d}\,(p^{3n} + p^{2n} + p^n + 1).$$

Any substitution T commutative with S has the canonical form, simultaneously with the canonical form of S,

$$T\colon\quad x' = \sigma^r x, \quad y' = \sigma^{rp^n} y, \quad z' = \sigma^{rp^{2n}} z, \quad w' = \sigma^{rp^{3n}} w,$$

where σ is a primitive root of the $GF[p^{4n}]$. But since the determinant is unity, we have

$$\sigma^{r(p^{3n}+p^{2n}+p^n+1)} = 1.$$

Hence r is a multiple of $p^n - 1$. Let $r = k(p^n - 1)$, then, since $\sigma^{p^{4n}-1} = 1$, we may choose $\lambda = \sigma^{p^n-1}$. Hence,

$$\sigma^r = \sigma^{k(p^n-1)} = \lambda^k,$$

so that $T = S^k$. Therefore, S is commutative only with its powers. Denoting by s the number of substitutions commutative with S in H, we have

$$s = p^{3n} + p^{2n} + p^n + 1,$$

while in G the number of commutative substitutions is $\frac{s}{d}$. Consequently, there are $\frac{M}{s}$ substitutions conjugate to S in H, and $\frac{Nd}{s} = \frac{M}{s}$ conjugate to S in G.

The substitutions S, S^{p^n}. $S^{p^{2n}}$, $S^{p^{3n}}$ are the only powers of S that have the same multipliers as S, and are, therefore, the only powers of S that are conjugate to it. Hence, there is one set of $\frac{M}{4s}$ conjugate cyclic subgroups in H of order s, and one set of $\frac{M}{4s}$ in G of order $\frac{s}{d}$.

Remark. The equality of the number of subgroups in the sets of H and of G occurs for most of the types, their orders consequently being in the ratio of d to 1.

To obtain the exact number of substitutions reducible to this type, i. e having an irreducible characteristic equation, we must exclude those powers of S and of its conjugates that have their multipliers in the $GF[p^{2n}]$. This will occur for S^m if $\lambda^{m(p^{2n}-1)} = 1$, hence

$$m(p^{2n}-1) = h(p^{3n}+p^{2n}+p^n+1),$$
$$m(p^n-1) = h(p^{2n}+1).$$

But $[p^n-1, p^{2n}+1] = [p^n-1, 2]$, which is unity when $d = 1$, and is 2, when $d = 2$ or 4. Therefore,

$$\text{for } d = 1, \quad m = h(p^{2n}+1), \quad (h = 1, 2, \ldots\ p^n+1),$$
$$\text{for } d = 2,\ 4, \quad m = \tfrac{1}{2}h(p^{2n}+1), \quad (h = 1, 2, \ldots\ 2(p^n+1)).$$

We therefore exclude $2j(p^n+1)$ substitutions from each subgroup of the set in H, and $\frac{2}{d}j(p^n+1)$ from each subgroup of the set in G, where $j = \frac{1}{2}$ if $d = 1$, and $j = 1$ if $d = 2$ or 4. There remain

$$s - 2j(p^n+1)$$

substitutions in each subgroup in H; altogether then

$$[s - 2j(p^n+1)]\frac{M}{4s}.$$

In G there will be left $\frac{1}{d}\,[s-2j\,(p^n+1)]$ substitutions in each cyclic subgroup; in all, therefore,

$$[s-2j\,(p^n+1)]\,\frac{N}{4s}$$

substitutions, each of period a factor of $\frac{s}{d}$, but not of p^n+1, when $d=1$, and not a factor of $2\,(p^n+1)$ when $d=2$ or 4.

Remark. The number of substitutions reducible to a given canonical form will be determined in every case, and their sum, which must be the order of the group may be calculated as a partial verification of the correctness of the work.

Type 2.

§9. A substitution of this type of determinant unity has the form

$$S:\quad x'=\lambda x,\quad y'=\lambda^{p^n}y,\quad z'=\lambda^{p^{2n}}z,\quad w'=\lambda^{-(p^{2n}+p^n+1)}w,$$

where λ is in the $GF[p^{3n}]$. Choosing λ to be a primitive root of that field, it follows that any substitution of this type is a power of S. The period of S is $p^{3n}-1$, and the period of the corresponding substitution in G is the least integer m such that

$$\lambda^m=\lambda^{mp^n}=\lambda^{mp^{2n}}=\lambda^{-m(p^{2n}+p^n+1)}.$$

Hence, $m\,(p^{2n}+p^n+2)=h\,(p^{3n}-1)$, where h is some integer. But

$$[p^{2n}+p^n+2,\ p^{3n}-1]=[4,\,p^n-1]=d,$$

so that $m=\frac{1}{d}\,(p^n-1)$.

The most general substitution T of determinant unity, commutative with S, is

$$T:\quad x'=\lambda^r x,\quad y'=\lambda^{rp^n}y,\quad z'=\lambda^{rp^{2n}}z,\quad w'=\lambda^{-r(p^{2n}+p^n+1)}.$$

Hence, $T=S^r$, so that S is commutative only with its powers. It results, then, that there are

$$M/(p^{3n}-1)$$

substitutions conjugate to S in both H and G. But S, S^{p^n}, $S^{p^{3n}}$ are the only powers of S conjugate to S, so there are $M/3\,(p^{3n}-1)$ distinct conjugate cyclic subgroups in the set for both groups.

The substitution S^t will have its characteristic equation further resolvable if

$$\lambda^{t(p^n-1)} = 1\,;$$

hence, $$t = h(p^{2n} + p^n + 1)\,, \quad h = (1, 2, \ldots . p^n - 1),$$

so that $(p^n - 1)$ powers of S will belong to other canonical forms. There remain $(p^{3n} - p^n)$ substitutions in each subgroup reducible to this canonical form. In all, then, there are in H

$$(p^{3n} - p^n)\, M/3\,(p^{3n} - 1)$$

substitutions, from this type, of period factors of $p^{3n} - 1$, but not factors of $(p^n - 1)$.

The group G evidently contains

$$(p^{3n} - p^n)\, N/3\,(p^{3n} - 1)$$

substitutions from this source, each of period a factor of $\frac{1}{d}(p^{3n} - 1)$, but not of period a factor of $\frac{1}{d}(p^n - 1)$.

Type 3.

§10.—We may choose λ a primitive root of the $GF\,[p^{2n}]$ in the substitution

$$S\colon \quad x' = \lambda x, \quad y' = \lambda^{p^n} y, \quad z' = \mu z, \quad w' = \mu^{p^n} w \qquad ((\lambda\mu)^{p^n+1} = 1\; \lambda \neq \mu).$$

The period of S is then $p^{2n} - 1$, while the period of S in G is the least integer m such that

$$\lambda^m = \lambda^{mp^n} = \mu^m = \mu^{mp^n}.$$

Hence m is a multiple of $p^n + 1$, say $m = h(p^n + 1)$. But since $(\lambda\mu)^{p^n+1} = 1$, μ is the $[-1 + k(p^n - 1)]^{\text{th}}$ power of λ. Hence

$$\mu^m = \lambda^{-m + km(p^n-1)} = \lambda^m.$$

Hence we have

$$2m - km(p^n - 1) \equiv 0, \qquad \pmod{p^{2n} - 1},$$
$$2h(p^n + 1) \equiv 0, \qquad \text{“}$$

Therefore, when $d = 1$, $h = p^n - 1$ and $m = p^{2n} - 1$; and when $d = 2$ or 4, $h = \frac{1}{2}(p^n - 1)$ and $m = \frac{1}{2}(p^{2n} - 1)$.

There are $p^n + 1$ values of μ given by

$$\mu = \lambda^{-1+k(p^n-1)}, \qquad (k = 1, 2, \ldots . p^n + 1).$$

But μ will be in the $GF[p^n]$ if

$$-1 + k(p^n - 1) \equiv 0, \qquad (\text{mod } p^n + 1),$$

which has a solution only when $p = 2$, viz. $k = 2^{n-1}$. Excluding this solution, there remain 2^n values of μ when $d = 1$ and $p^n + 1$, when $d = 2$ or 4. These will give rise to substitutions conjugate in pairs, since, for every value of μ, μ^{p^n} is also in the list given by the values k and $p^n - k$ respectively. Hence, when $d = 1$, there are 2^{n-1} distinct sets of conjugate cyclic subgroups, and when $d = 2$ or 4, there are $\frac{1}{2}(p^n + 1)$ such sets. (The cases $p^n = 2$ and $p^n = 3$ are exceptions, there being no set for the former and only one for the latter.)

The most general substitution T for this type is

$$T\colon\quad x' = \lambda^r x, \quad y' = \lambda^{rp^n} y, \quad z' = \lambda^s z, \quad w' = \lambda^{sp^n} w,$$

where $\lambda^{(r+s)(p^n+1)} = 1$. Hence, there are $p^n + 1$ values of λ^{r+s}, and for each of these, r may take $p^{2n} - 1$ values and s is then determined, so that there are $(p^n + 1)(p^{2n} - 1)$ substitutions commutative with one of this type. There are then in G

$$M/(p^n + 1)(p^{2n} - 1)$$

substitutions conjugate to S.

Putting $t = -1 + k(p^n - 1)$, the multipliers of S may be written λ, λ^{p^n}, λ^t, λ^{tp^n}. It is seen that S and S^{p^n} are conjugates. Further, they will also be conjugate to S^t and S^{tp^n} if

$$t^2 \equiv 1 \quad \text{or} \quad t^2 \equiv p^n, \qquad (\text{mod } p^{2n} - 1).$$

The first congruence becomes

$$(2k + 1)^2 \equiv 1, \qquad (\text{mod } 2(p^n + 1)),$$

which has $2^{j+\tau}$ distinct solutions, where j is the number of odd prime factors of $2(p^n + 1)$, and if 2^h is the highest power of 2 contained in $2(p^n + 1)$, then $\tau = 0$ if $h = 1$; $\tau = 1$ if $h = 2$; $\tau = 2$ if $h > 2$. (Dirichlet, "Zahlentheorie," §37.)

These $2^{j+\tau}$ solutions for $2k + 1$ may be taken positive and $< 2(p^n + 1)$ and hence give $k \leqq p^n + 1$, so that all must be considered. The corresponding sets, however, will coincide in pairs, for if k is one solution of the congruence $p^n - k$ is also a solution. Hence, just $2^{j+\tau-1}$ sets arise such that powers of the generators of the cyclic subgroups composing them are conjugate by fours.

The other congruence becomes

$$(2k+1)^2 \equiv -1, \qquad (\mathrm{mod}\ 2(p^n+1)),$$

and has solutions only for $p=2$, $d=1$; it then becomes

$$(2k+1)^2 \equiv -1, \qquad (\mathrm{mod}\ 2^n+1).$$

But -1 is a residue only of primes of the form $4l+1$. Hence, when 2^n+1 has all its prime factors, j in number, of the form $4l+1$, 2^j solutions occur. These lead to 2^{j-1} sets in our group H.

When $d=1$, therefore, there are g sets of conjugate cyclic subgroups such that any generator is conjugate with four of its powers, where g is $2^{j+\tau-1}+2^{j-1}$, if all the odd prime factors of 2^n+1 are of the form $4l+1$, and g is equal to $2^{j+\tau-1}$ in all other cases. The remaining $2^{n-1}-g$ sets are such that the generators are conjugate with just two of their powers. Hence, in H and in G we have, for $d=1$, g sets each containing

$$M/4(p^n+1)(p^{2n}-1)$$

conjugate cyclic subgroups, and $2^{n-1}-g$ sets each containing

$$M/2(p^n+1)(p^{2n}-1)$$

subgroups; every subgroup being of order $2^{2n}-1$.

When $d=2$ or 4, just $2^{j+\tau-1}$ sets are such that every generator is conjugate with four of its powers, the remaining

$$\tfrac{1}{2}(p^n+1)-2^{j+\tau-1}$$

sets have each generator conjugate with only two of its powers. In H, every group of these sets is of order $p^{2n}-1$.

§11.—In passing from H to G, it must be noticed in each type whether or not S is conjugate with $\Theta^i S$; Θ being the substitution that multiplies every index by θ, a primitive fourth root of unity. In general, if the multipliers of the canonical form of a substitution W are M_1, M_2, M_3, M_4, then those of $\Theta^i W$ are $\theta^i M_1$, $\theta^i M_2$, $\theta^i M_3$, $\theta^i M_4$; and if W is conjugate with $\Theta^i W$, then the two substitutions have the same set of multipliers, apart from their order. Since the determinant of the substitution is unity, we have

$$M_1 M_2 M_3 M_4 = 1.$$

Suppose $\theta^i M_1 = M_2$, then if $\theta^i M_2 = M_1$, $\theta^{2i} = 1$ or $i = 2$; and since $\theta^2 M_3 \neq M_3$, we have $\theta^2 M_3 = M_4$. Hence,

$$M_1\, \theta^2 M_1\, M_3\, \theta^2 M_3 = 1, \text{ or } M_3 = \frac{1}{M_1}, \text{ or } M_3 = \frac{\theta^2}{M_1}.$$

The multipliers are then M_1, $\theta^2 M_1$, $\frac{1}{M_1}$, $\frac{\theta^2}{M_1}$.

If $\theta^i M_2 \neq M_1$, then we must have, by properly choosing the notation, $\theta^i M_2 = M_3$. Hence, the multipliers become M_1, $\theta^i M_1$, $\theta^{2i} M_1$, $\theta^{3i} M_1$ $(i = 1, 2, 3, 4)$. Hence, $M_i^4 = -1$. These are the only two possible sets of multipliers such that W and $\theta^i W$ are conjugates.

In the first case, W and $\Theta^2 W$ would be conjugates and would correspond to the same substitution in G, so that the set of substitutions conjugate to W in H must be divided by two in passing to the group G. If W has the second set of multipliers, then the number of substitutions conjugate to W in H reduces to one-fourth that number for the corresponding set in G.

If $\Theta^i W$ is conjugate with some power of W, for j values of i $(j \leqq 4)$, then the number of subgroups conjugate to the group $\{W\}$ will be reduced in the ratio $\frac{1}{j}$ in passing to the group G. Should it happen that $\Theta^i W$ lies in a set of conjugate cyclic subgroups distinct from the one in which W lies, there will be a corresponding union of sets in G. Since i may be equal to four, both of these latter cases may occur simultaneously, as will happen in type 3 under consideration [cf. §12].

§12.—The multipliers of the typical generator S being λ, λ^{p^n}, λ^t, λ^{tp^n}, where $t = -1 + k(p^n - 1)$, it is seen that they do not fulfill the first conditions of §11. However, it will happen that in passing from H to G some of the sets will coincide when $d = 4$.

There will be the same number of sets in both H and G when $d = 2$, each set containing the same number of conjugate subgroups in the two groups, the orders, however, being $\frac{1}{2}(p^{2n} - 1)$ in the group G. This may be verified by noticing that $\Theta^2 S$ is S raised to the power $\frac{1}{2}(p^{2n} + 1)$.

When $d = 4$, ΘS and $\Theta^3 S$ are not conjugate with powers of S in all cases, and they will be shown in these cases to lie in a set distinct from the one of which S is the typical generator. Hence, in passing from H to G, these two sets unite into one.

To determine the number of such cases, consider when the multipliers of ΘS are the same as those of some power of S. Since $\theta = \lambda^{\frac{1}{4}(p^{2n}-1)}$, the multipliers of ΘS are λ raised to the following powers:

$$\tfrac{1}{4}(p^{2n}+3), \quad p^n + \tfrac{1}{4}(p^{2n}-1), \quad t + \tfrac{1}{4}(p^{2n}-1), \quad tp^n + \tfrac{1}{4}(p^{2n}-1).$$

It will be sufficient to consider S to the powers $\frac{1}{4}(p^{2n}+3)$ and $t + \frac{1}{4}(p^{2n}-1)$, for, if ΘS is conjugate to S^m, it will be conjugate to S^{mp^n}.

The first two multipliers in S to the power $t + \frac{1}{4}(p^{2n}-1)$ coincide with the last two in ΘS. The third will be equal to the first in ΘS if

$$t^2 + \tfrac{1}{4}t(p^{2n}-1) \equiv \tfrac{1}{4}(p^{2n}+3), \qquad [\bmod p^{2n}-1],$$

or

$$-2k(k+1) + \tfrac{1}{2}(p^n+1)[-1 + \frac{k}{2}(p^n-1)] \equiv 0, \quad [\bmod p^n+1].$$

Since, for $d = 4$, p^n+1 is of the form $2(2l+1)$, this congruence has no solutions, being of the form

$$A + B \equiv 0, \qquad [\bmod 2(2l+1)],$$

where A is even and B is odd.

The other possibility is that the third multiplier be equal to the second one of ΘS, which gives the condition

$$t^2 + \frac{t}{4}(p^{2n}-1) \equiv p^n + \tfrac{1}{4}(p^{2n}-1), \qquad [\bmod (p^{2n}-1)].$$

Substituting for t its value $-1 + k(p^n-1)$, this becomes

$$-(1+2k+2k^2) + \tfrac{1}{2}(p^n+1)[-1 + \tfrac{1}{2}k(p^n-1)] \equiv 0, \quad [\bmod p^n+1].$$

It is, therefore, necessary and sufficient that $1 + 2k + 2k^2$ be an odd multiple of $\frac{1}{2}(p^n+1)$. The congruence

$$2k^2 + 2k + 1 \equiv 0 \qquad [\bmod \tfrac{1}{2}(p^n+1)]$$

becomes

$$(2k+1)^2 \equiv -1, \qquad [\bmod p^n+1].$$

Since -1 is a residue only of primes of the form $4r+1$, it is necessary that all the odd prime factors of p^n+1 shall be of the form $4r+1$. We will call τ the number of solutions of this congruence that give rise to distinct sets of conjugate subgroups, where τ, if it exists, is an even integer.

Example.—If $p^n = 9$, the above congruence becomes

$$2k^2 + 2k + 1 \equiv 0, \qquad (\bmod 5).$$

Then p^n+1, having the single odd prime factor 5, has solutions, viz. $k = 1$ and

$k=3$. The corresponding substitutions are seen to have the property stipulated.

The other possibility is that the multipliers of ΘS are the same as those of $S^{\frac{1}{4}(p^{2n}+3)}$. The multipliers of the latter are λ raised to the following powers:

$$\tfrac{1}{4}(p^{2n}+3),\quad \tfrac{1}{4}p^n(p^{2n}+3),\quad \tfrac{1}{4}t(p^{2n}+3),\quad \tfrac{1}{4}tp^n(p^{2n}+3).$$

The first two multipliers are the same for the two substitutions, the first ones obviously, the second ones because

$$p^n+\tfrac{1}{4}(p^{2n}-1)\equiv\tfrac{1}{4}p^n(p^{2n}+3), \qquad [\mathrm{mod}\ (p^{2n}-1)],$$

which reduces to

$$p^n-1\equiv 0, \qquad (\mathrm{mod}\ 4),$$

which is true, since $p^n=4l+1$. $(d=4)$.

The third multipliers of each will be identical if

$$t+\tfrac{1}{4}(p^{2n}-1)\equiv t\,.\,\tfrac{1}{4}(p^{2n}+3), \qquad [\mathrm{mod}\ p^{2n}-1],$$

Putting $t=-1+k(p_n-1)$, this reduces to

$$k(p^n-1)\equiv 2, \qquad [\mathrm{mod}\ 4],$$

which is not satisfied, since $p^n-1\equiv 0$ (mod 4).

It must then happen that the third multiplier of the first set coincides with the fourth one of the second set, and vice versa. This will be so if

$$t+\frac{p^{2n}-1}{4}\equiv p^n\,.\,t\tfrac{1}{4}(p^{2n}+3), \qquad [\mathrm{mod}\ p^{2n}-1],$$

which reduces to

$$8k+4+(p^n+1)^2-(p^n+1)[kp^n(p^n-1)+4k]\equiv 0, \qquad [\mathrm{mod}\ 4(p^n+1)],$$

It is, therefore, necessary and sufficient that

$$4(2k+1)+(p^n+1)^2\equiv 0, \qquad [\mathrm{mod}\ 4(p^n+1)],$$

which requires that

$$4(2k+1)\equiv 0, \qquad [\mathrm{mod}\ p^n+1].$$

Since p^n has the form $4l+1$ in this case, $(d=4)$, this may be written

$$2(2k+1)\equiv 0, \qquad [\mathrm{mod}\ 2l+1],$$

the only solutions of which, $k\overline{<}p^n+1$, are

$$k=l \quad\text{and}\quad k=3l+1=p^n-l.$$

But, from §10, these two values of k give rise to the same set of conjugate substitutions. Furthermore, these values of k cannot satisfy the congruence [§10]

$$(2k+1)^2 \equiv 1, \qquad [\operatorname{mod} 2(p^n+1)],$$

so that the powers of the generating substitutions in this set are conjugate only by twos.

§13.—When $d = 4$, there will be $\tau + 1$ sets of conjugate cyclic subgroups such that if S is a typical generator, $\Theta^i S$ ($i = 1, 2, 3, 4$) all lie in the set of which the group $\{S\}$ is a member, τ being zero unless all the prime factors of $p^n + 1$ are of the form $4r + 1$. It has been shown that $\Theta^2 S$ is a power of S, hence, ΘS and $\Theta^3 S$ are powers of a certain substitution conjugate to S, so that in the group G the subgroups of these sets, and their orders are just half what they are in the group H. Since there are

$$M/2\,(p^n+1)(p^{2n}-1)$$

subgroups in each of these sets in H, there will be in G, $\tau + 1$ sets having

$$M/4\,(p^n+1)(p^{2n}-1)$$

conjugate cyclic subgroups, each of order $\frac{1}{2}(p^{2n}-1)$.

There remain in H, $\frac{1}{2}(p^n-1) - \tau$ sets such that the typical substitution S and ΘS lie in different sets, which, therefore, coincide in G [cf. §11], producing

$$\tfrac{1}{4}(p^n-1) - \frac{\tau}{2}$$

sets for that group. From the latter part of §10 it follows that of these sets $2^{j+\tau-3}$ will contain

$$M/4\,(p^n+1)(p^{2n}-1)$$

cyclic subgroups, while the remainder will have

$$M/2\,(p^n+1)(p^{2n}-1)$$

subgroups, the order of the subgroups being in all cases $\frac{1}{2}(p^{2n}-1)$.

§14.—*Determination of total number of substitutions reducible to type* 3.

We need only to consider the number of values of λ and μ such that $(\lambda\mu)^{p^n+1} = 1$ ($\lambda \neq \mu$, $\lambda \neq \mu^{p^n}$), and such that each pair of values gives rise to a distinct set of $M/(p^n+1)(p^{2n}-1)$ conjugate substitutions.

(i) $d = 1$. In this case $p = 2$. For every value of λ in the $GF[p^{2n}]$, μ takes $p^n + 1$ values, one of which, by §10, is in the $GF[p^n]$ and is to be excluded. If σ is a primitive root of the $GF[p^{2n}]$ and

$$\lambda = \sigma^{-h(p^n-1)}, \qquad (h = 1, 2, \ldots . p^n).$$

μ may have the values $\sigma^{h(p^n-1)}$ and $\sigma^{hp^n(p^n-1)}$, which must be excluded, since then λ will be equal to μ or μ^{p^n}. Hence, for these p^n values of λ, μ takes only $p^n - 2$ values. For the remaining $p^{2n} - 2p^n$ values of λ not in the $GF[p^n]$, μ may take p^n values so that, in all, there are

$$(p^{2n} - 2p^n)p^n + p^n(p^n - 2) = p^n(p^n + 1)(p^n - 2)$$

values of λ and μ to be considered. The substitutions arising from these sets of values will, however, be conjugate in sets of eight, so that there are

$$\tfrac{1}{8}p^n(p^n + 1)(p^n - 2)$$

distinct sets, each containing

$$M/(p^n + 1)(p^{2n} - 1)$$

distinct conjugate substitutions, each of period a factor of $p^{2n} - 1$ but not of $p^n - 1$.

(ii) $d = 2$ or 4. Let $\lambda = \sigma^t$, then the values of μ are given by

$$\mu = \sigma^{-t + k(p^n-1)}, \qquad (k = 1, 2, \ldots . p^n + 1).$$

But μ will be in the $GF[p^n]$ if

$$-t + k(p^n - 1) \equiv 0, \qquad (\text{mod } p^n + 1),$$

and since $p^n + 1$ is even, this congruence requires that t be even and that

$$2k + t \equiv 0, \qquad (\text{mod } p^n + 1),$$

giving two values of k, $0 < k \leqq p^n + 1$. Hence, for each of the $\frac{1}{2}(p^{2n} - 1)$ values of λ equal to an odd power of σ, μ may take $p^n + 1$ values, making in all $\frac{1}{2}(p^{2n} - 1)(p^n + 1)$.

There are $\frac{1}{2}(p^{2n} - 1) - (p^n - 1) = \frac{1}{2}(p^n - 1)^2$ even powers of σ not in the $GF[p^n]$, and for each of these μ takes $p^n - 1$ values, making in all $\frac{1}{2}(p^n - 1)^3$. The equation

$$\lambda^{2(p^n+1)} = 1$$

has $2(p^n + 1)$ solutions in the $GF[p^{2n}]$, viz.

$$\lambda = \sigma^{k'\frac{p^n-1}{2}}, \qquad (k' = 1, 2, \ldots . 2(p^n + 1)),$$

When $d = 2$, the solutions given by $k' = p^n + 1$ and $k' = 2(p^n + 1)$ are in the $GF[p^n]$, and when $d = 4$, there are besides these the solutions $k' = \frac{1}{2}(p^n + 1)$ and $k' = \frac{3}{2}(p^n + 1)$. Hence, there are $2(p^n + 1) - d$ solutions not in the $GF[p^n]$. To each one of these solutions correspond two sets of multipliers such that either $\lambda = \mu$ or $\lambda = \mu^{p^n}$, so that we exclude $4(p^n + 1) - 2d$ of the above solutions, leaving

$$\tfrac{1}{2}(p^{2n} - 1)(p^n + 1) + \tfrac{1}{2}(p^n - 1)^3 - 4(p^n + 1) + 2d,$$

or
$$(p^n - 1)(p^{2n} + 1) - 4(p^n + 1) + 2d$$

sets of solutions λ, μ, which give rise to substitutions conjugate in sets of eight. There are then one-eighth this number of distinct sets of conjugate substitutions of this type for $d = 2$ or 4, each set containing

$$M/(p^n + 1)(p^{2n} - 1)$$

substitutions.

The discussion of §12 shows that to find the number of sets of conjugate substitutions for the group G arising from this type, we need only to divide the number for H, just found, by d, the sets containing the same number of substitutions as those in the group H.

Type 4 (i).

§15.—The general substitution of this canonical form is

$$S:\quad x' = \lambda x, \quad y' = \lambda(y + x), \quad z' = \lambda^{p^n} z, \quad w' = \lambda^{p^n}(w + z),$$

where $\lambda^{2(p^n+1)} = 1$. When $d = 1$, we may choose λ to be a primitive root of the equivalent equation $\lambda^{p^n+1} = 1$. The period of S will then be $p(p^n + 1)$ when $d = 1$. Denoting by σ a primitive root of the $GF[p^{2n}]$, we may write the most general commutative substitution T in the form

$$x' = \sigma^r x, \quad y' = \sigma^s x + \sigma^t y, \quad z' = \sigma^{rp^n} z, \quad w' = \sigma^{sp^n} z + \sigma^{rp^n} w,$$

where $\sigma^{2r(p^n+1)} = 1$, which has for $d = 1$ $p^{2n(p^n+1)}$ solutions. Consequently, for $d = 1$ there are

$$M/p^{2n}(p^n + 1)$$

conjugate with S. But S and $S^{-1} = S^{2p^n+1}$ are conjugate substitutions, so that there is one set of

$$M/2p^{2n}(p^n + 1)$$

conjugate cyclic subgroups.

The substitution S^{p^n+1} has all its multipliers in the $GF[p^n]$, while those of the form

$$S^{2h}.\,(h = 1,\ 2,\ \ldots .\ p^n + 1)$$

are of type 4 (ii), leaving only p^n powers of S and of the generators of the cyclic subgroups conjugate to the group $\{S\}$, that belong to this canonical form. Hence, when $d = 1$, there are in H and in G

$$M/2p^n(p^n+1)$$

substitutions reducible to this type.

When $d = 2$ or 4, we may choose λ to be a primitive root of the equation

$$\lambda^{2(p^n+1)} = 1,$$

so that S is of period $2p(p^n+1)$, and any substitution of this canonical form is conjugate with some power of S, just as for $d = 1$. Hence, there is again a single set of conjugate cyclic subgroups.

If we have

$$m = 2k(p^n+1)+1, \qquad (k = 1,\ 2,\ \ldots .\ p\,;\ 2k \not\equiv -1 \pmod{p}),$$

then S and S^m are conjugates. Indeed, the substitution

$$W\colon\ x' = \mu x,\quad y' = \sigma x + \mu m^{-1} y,\quad z' = \mu^{p^n} z,\quad w' = \sigma^{p^n} z + \mu^{p^n} m^{-1} w,$$

transforms S^m into S, and since the determinant of W is $\mu^{2(p^n+1)}m^{-2}$, it may be chosen equal to unity, μ being arbitrary in the $GF[p^{2n}]$ and m not being divisible by p.

In the same way it may be shown that S is conjugate with $p-1$ other powers, the exponents of which are of the form

$$p^n + 2h(p^n+1), \qquad (h = 1,\ 2,\ \ldots .\ p),$$

where we exclude the one divisible by p. Altogether, then, S is conjugate with $2(p-1)$ of its powers, and since, for $d = 2$ or 4, there are $2p^{2n}(p^n+1)$ substitutions T commutative with S, it results that there are

$$M/4(p-1)p^{2n}(p^n+1)$$

conjugate subgroups in the set.

In determining the number of substitutions in H reducible to this canonical form for $d = 2$ or 4, we must exclude the $2(p^n+1)$ powers of the generators of the cyclic groups of the set whose exponents are multiples of p; and also the

$d(p-1)$ powers of S whose exponents are of the form $\frac{2k(p^n+1)}{d}$ that are not contained amongst the above $2(p^n+1)$ excluded powers. There remain

$$2p(p^n+1)-2(p^n+1)-d(p-1)=(p-1)[2(p^n+1)-d]$$

powers of each generator that belong to this canonical form. Altogether, there are, for $d=2$ or 4,

$$(2(p^n+1)-d)\,M/4p^{2n}(p^n+1)$$

substitutions in H reducible to this type, their periods being factors of $2p(p^n+1)$ but not factors of $2p$ or $2(p^n+1)$.

The period of S in G is the least integer pr such that

$$\lambda^r=\lambda^{rp^n} \quad \text{or} \quad \lambda^{r(p^n-1)}=1.$$

Since $[p^n-1,\ 2(p^n+1)]=d$, it follows that $r=\frac{2}{d}(p^n+1)$. Hence, the period is $\frac{2}{d}\,p(p^n+1)$, it being so that d powers of each generator in H unite to form a single substitution in G, the number of subgroups in the set remaining unchanged. There are, therefore, in G

$$\frac{1}{d}(p-1)[2(p^n+1)-d]$$

substitutions in each of the subgroups that arise from this canonical form.

Type 4′ (i).

§16.—Since the substitutions of this type are conjugate in the general homogeneous group with those of type 4 (i) by means of a substitution of determinant a particular not-square t, it follows that the two types present the same arrangement as to conjugate cyclic subgroups. Indeed, if $S^{(\nu)}$ represents the substitutions of 4 (i) and W is a properly chosen substitution of determinant t, then $S_1^{(\nu)}=W^{-1}S^{(\nu)}W$ represents the substitutions of 4′ (i) as $S^{(\nu)}$ runs through its list. The substitutions $S_1^{(\nu)}$ being distinct, we see that there are the same number of substitutions for the two types.

Type 4 (ii).

§17.—The general substitution S of this type is

$$x'=\lambda x,\quad y'=\lambda y,\quad z'=\lambda^{p^n}z,\quad w'=\lambda^{p^n}w,\qquad (\lambda^{2(p^n+1)}=1).$$

Just as in type 4 (i), we choose λ to be a primitive root of the equations

$$\lambda^{(p^n+1)}=1, \quad \lambda^{2(p^n+1)}=1,$$

according as $d=1$ or $d=2$ or 4 respectively. The substitution S is then of period p^n+1 or $2(p^n+1)$, as the case may be, and every substitution of this canonical form is a power of S, so that there is a single set of conjugate cyclic subgroups.

The most general substitution T in this case is

$$x'=ax+by, \quad y'=cx+gy, \quad z'=a^{p^n}z+b^{p^n}w, \quad w'=c^{p^n}z+g^{p^n}w,$$

a, b, c, g being marks of the $GF[p^{2n}]$ and $\tau^{p^n+1}=1$, where $\tau=ag-bc$. Then $\tau^{p^n+1}=1$ has p^n+1 solutions in the $GF[p^{2n}]$. But for a particular value of τ, the equation $ag-bc=\tau$ has $p^{2n}(p^{4n}-1)$ solutions. Hence, there are $p^{2n}(p^n+1)(p^{4n}-1)$ substitutions commutative with S, and, consequently,

$$M/p^{2n}(p^n+1)(p^{4n}-1)$$

conjugate with it.

Since S^{p^n} is the only power of S conjugate to S, there is in the set in H

$$M/2p^{2n}(p^n+1)(p^{4n}-1)$$

conjugate cyclic subgroups, and since the period of S in G is $\frac{2}{d}(p^n+1)$ for $d=2, 4$, the set in G will also contain this many subgroups.

Excluding the identity, the set contains, when $d=1$,

$$M/2p^n(p^n+1)(p^{4n}-1)$$

substitutions reducible to this type, viz. the p^n powers of S, not the identity, and their conjugates. When $d=2$ or 4, each group of the set contains $2(p^n+1)-d$ substitutions reducible to this canonical type, viz. those powers of each generator whose multipliers have not one of the d values 1, -1, θ, θ^3.

Type 5.

§18.—Consider the substitution S of this type when λ is a primitive root of the $GF[p^{2n}]$, viz.

$$S\colon \quad x'=\alpha x, \quad y'=\beta y, \quad z'=\lambda z, \quad w'=\lambda^{p^n}w, \qquad (\alpha\beta\lambda^{p^n+1}=1,\ \alpha\neq\beta).$$

If $\alpha=\rho^r$, where $\rho=\lambda^{p^n+1}$ is a primitive root of the $GF[p^n]$, then $\beta=\rho^{-1-r}$. We will have $\alpha=\beta$ if

$$2r+1\equiv 0, \qquad (\mathrm{mod}\ p^n-1),$$

which has a solution only when $p = 2$, i. e. $d = 1$, viz. $r = \frac{1}{2}(p^n - 2)$. Excluding this value which comes under type 6 (ii), r may take $\frac{1}{2}(p^n - 2)$ values, each giving rise to a distinct set of conjugate cyclic subgroups of order $(p^{2n} - 1)$. For $d = 2$ or 4, there are evidently $\frac{1}{2}(p^n - 1)$ such sets.

The most general substitution T is

$$x' = ax, \quad y' = by, \quad z' = \lambda^s z, \quad w' = \lambda^{sp^n} w, \qquad [ab\lambda^{s(p^n+1} = 1].$$

with $(p^n + 1)(p^n - 1)^2$ distinct forms, so that there are

$$M/(p^n + 1)(p^n - 1)^2$$

substitutions conjugate with one of this type. In the substitution under consideration, S and S^{p^n} are the only powers of S that are conjugates. Hence, in each of the above sets there are

$$M/2(p^n + 1)(p^n - 1)^2$$

cyclic subgroups.

The most general substitution of this canonical form is

$$U: \quad x' = \rho^t x, \quad y' = \rho^{-t-h} y, \quad z' = \lambda^h z, \quad w' = \lambda^{hp^n} w.$$

We will have $U = S^h$ if

$$rh \equiv t, \qquad \pmod{p^n - 1},$$

which can be solved for r, provided $[h, p^n - 1]$ is a factor of t. When this condition is not satisfied, sets will arise whose structure may be best studied for particular fields. They will, therefore, be omitted here.

The period of S as a substitution of the group G is the least integer m such that

$$\rho^{rm} = \rho^{-m(r+1)} = \lambda^m = \lambda^{mp^n}.$$

Hence, m is a multiple of $p^n + 1$, say $k(p^n + 1)$. Then, since $\lambda^{p^n+1} = \rho$, we must have, modulo $p^n - 1$,

$$k(p^n + 1)(2r + 1) \equiv 0, \quad rk(p^n + 1) - k \equiv 0.$$

Hence, $$2k(2r + 1) \equiv 0, \quad k(2r - 1) \equiv 0,$$

which gives the condition $k \equiv 0$ modulo $p^n - 1$. The least value m is then $p^{2n} - 1$, hence the periods of S in H and of S in G being the same, it follows that d substitutions in H unite into one in G, all lying in different subgroups. There will be, then, either a union of d sets into one or a union of d subgroups of the same set into one subgroup, or when $d = 4$, perhaps a combination of both cases will occur, two sets uniting to form one with half as many subgroups [cf. §11]. Similar properties should be expected also for the cyclic subgroups of this type not included among those of which S is the typical generator.

§19.—*Examples.* As illustrations of what happens for this type, consider some particular fields.

(i) $p^n = 4 \,.\, (d = 1)$. There is one substitution S of period 15 with multipliers $1, \rho^2, \lambda, \lambda^4$. The substitution V with multipliers $\rho, \rho^2, \lambda^3, \lambda^5$ is not a power of S, and generates a cyclic group of order 15. There are in this case two sets of conjugate cyclic subgroups of which S and V are the typical generators.

(ii) $p^n = 3 \,.\, (d = 2)$. For this case, there is one set of subgroups the typical generator S of period 8, having the multipliers $1, \rho, \lambda, \lambda^3$. Since $\Theta^2 S$ is conjugate with S^5, the set in G contains one-half as many subgroups as the sets in H, the groups in both sets being of order 8.

(iii) $p^n = 5 \,.\, (d = 4)$. There are two substitutions S for this case, viz. $(1, \rho^3, \lambda, \lambda^5)$ and $(\rho, \rho^2, \lambda, \lambda^5)$ of period 24. Calling them S_1 and S_2, we see that $\Theta^2 S_1$ is conjugate with S_2^{13} and that ΘS_i and $\Theta^3 S_i$ are conjugate respectively with S_i^7 and S_i^{19}. Hence, the two sets, of which S_1 and S_2 are the typical generating substitutions, coincide in G and the resulting set contains one-half as many subgroups as each of the distinct sets in H contain. Besides S_1 and S_2, H contains the substitution $(\rho, \rho^3, \lambda^4, \lambda^{20})$, which is not contained in the cyclic groups $\{S_1\}$ and $\{S_2\}$. The corresponding set in G is merged into the set resulting from the union of S_1 and S_2.

§20.—In order to determine the arrangement of the substitutions of type 5 into complete sets of conjugate substitutions, and hence find the total number of substitutions reducible to this type, we determine all the solutions of the equation

$$\alpha\beta\lambda^{p^n+1} = 1$$
$$(\alpha \neq \beta,\ \lambda \text{ in the } GF[p^{2n}],\ \text{not in } GF[p^n])$$

that lead to non-conjugate substitutions of the type.

Since λ takes $p^{2n} - p^n$ values not in the $GF[p^n]$ and β may take $p^n - 1$ values not equal to zero, there are $(p^n - 1)(p^{2n} - p^n)$ solutions, including those for $\alpha = \beta$. But the equation

$$\alpha^2\lambda^{p^n+1} = 1$$

gives p^n+1 values for each of the p^n-1 values of α $(\alpha \neq 0)$, one of which is in the $GF[p^n]$ when $d=1$, and two when $d=2$ or 4. Hence, we must exclude $p^n(p^n-1)$ substitutions when $d=1$ and $(p^n-1)^2$ when $d=2$ or 4, the excluded ones being exactly those that occur in type 6 (i). There remain, accounting for permutations,

$$\tfrac{1}{4}p^n(p^n-1)(p^n-2)$$

solutions for $d=1$ and

$$\tfrac{1}{4}(p^n-1)^3$$

for $d=2$ or 4, which lead to non-conjugate substitutions of this canonical form, each of which is one of a set of $M/(p^n+1)(p^n-1)^2$ distinct conjugate substitutions.

Type 6 (i).

§21.—There exists a substitution

$$S:\quad x'=\alpha x,\quad y'=\alpha y,\quad z'=\lambda z,\quad w'=\lambda^{p^n}w,\qquad [\alpha^2\lambda^{p^n+1}=1],$$

with λ a primitive root of the $GF[p^{2n}]$. In the case $d=1$, α is uniquely determined by this choice of λ, and furthermore, every substitution of the type is a power of S. For, consider the most general substitution

$$W:\quad x'=\rho^r x,\quad y'=\rho^r y,\quad z'=\lambda^k z,\quad w'=\lambda^{kp^n}w,$$

where $\rho=\lambda^{p^n+1}$. Since the determinant is unity, we have $\rho^{2r}=\rho^{-k}$. But S^k has the multipliers α^k, α^k, λ^k, λ^{kp^n}, where $\alpha^{2k}=\rho^{-k}$. Hence, $\alpha^{2k}=\rho^{2k}$ which gives $\alpha^k=\rho^r$ when $d=1$, so that $W=S^k$. There will then be a single set of conjugate cyclic subgroups in this case.

The most general substitution T for this type is

$$x'=ax+by,\quad y'=cx+gy,\quad z'=\lambda z,\quad w'=\lambda^{p^n}w,$$

which can be set up in $p^n(p^{2n}-1)^2$ distinct ways. Since S and S^{p^n} are the only powers of S conjugate to S, the set contains

$$M/2p^n(p^{2n}-1)^2$$

conjugate cyclic subgroups of order $p^{2n}-1$, each group containing $p^{2n}-p^n$ substitutions reducible to this canonical form.

When $d=2$ or 4, the substitution S as taken above does not exist, since λ^{p^n+1} is a not-square in the $GF[p^n]$. Keeping λ a primitive root of the

$GF[p^{2n}]$, we now choose S to be the substitution,

$$x' = \alpha x, \quad y' = \alpha y, \quad z' = \lambda^2 z, \quad w' = \lambda^{2p^n} w, \qquad (\alpha^2 \lambda^{2(p^n+1)} = 1).$$

We therefore have $\alpha = \pm \rho^{-1}$. Calling A the substitution with $\alpha = +\rho^{-1}$ and B the one with $\alpha = -\rho^{-1}$, we see that for the homogeneous group, both A and B are of period $\frac{1}{2}(p^{2n} - 1)$. Furthermore, there exist the relations

$$A^2 = B^2, \quad AB = BA.$$

The cyclic subgroups may be determined by applying the results for the abstract commutative group, which will next be investigated.

§22.—*Determination of the cyclic subgroups of the abstract group defined by the relations*

$$A^m = B^m = 1, \quad AB = BA, \quad A^2 = B^2.$$

No non-cyclic group exists for m an odd integer, for in that case $A^{m+1} = B^{m+1}$, or $A = B$. Assume then that m is even (as it is in type 6 (i)). Suppose, first, that $m = 2m'$, when m' is odd. The cyclic group $\{A\}$ contains all the operators of the form A^t, and $\{B\}$ will have, besides those of the form A^{2t}, all of the form $A^{2t}B$. There remain only those of the type $A^{4t\pm 1}B$, which will be present in the group $\{AB\}$. The latter of which is also of order m, when $m = 2m'$, m' odd.

Suppose next that $m = 4m'$, where m' is odd. The cyclic subgroups $\{A\}$ and $\{B\}$ are the same as before; but, since $(AB)^{2m'} = A^{4m'} = 1$, the group $\{AB\}$ is of order $2m'$, and does not contain the operators of the form A^{4t-1}. We must, therefore, have an additional subgroup $\{A^3B\}$ which is of order $\frac{m}{2}$, and contains all the operators of the form $A^{4t-1}B$; for

$$(A^3B)^{2r+1} = A^{8r+3}B,$$

and

$$A^{8r+3} = A^{8r+3-4m'} = A^{8r'-1}, \qquad \left(r' = r - \frac{m'-1}{2}\right).$$

In general, if $m = 2^k m'$, where m' is odd, the smallest number of cyclic subgroups which include all the operators is $k + 2$. For example, $\{A\}$, $\{B\}$ of order m, and

$$\{A^{2^j-1}B\} \qquad (j = 1, 2, \ldots . k)$$

of order $\frac{m}{2^j}$ respectively, excepting $\{A^{2^k-1}B\}$, which is of order $\frac{m}{2^{k-1}}$. To prove this latter statement, suppose that

$$\{A^{2^j-1}B\}^{2t} = A^{2^{j+1}\cdot t} = 1.$$

This will be true if

$$t\,.\,2^{j+1} \equiv 0, \qquad (\text{mod } 2^k m').$$

Hence,

$$t \equiv 0, \qquad (\text{mod } 2^{k-j-1} m').$$

For $j < k$, the least value of $2t$ satisfying this condition is seen to be $\frac{m}{2^j}$, and for $j = k$ it is $\frac{m}{2^{k-1}}$.

§23.—For the subgroups of type 6 we have

$$m = \tfrac{1}{2}(p^{2n} - 1),$$

and since $p^n = 4l \pm 1$, it results that

$$m = 4l(2l \pm 1),$$

so that there are at least four cyclic subgroups.

The multipliers of $A^{2^j-1}B$ being

$$-\rho^{-2^j}, \quad -\rho^{-2^j}, \quad \lambda^{2^j+1}, \quad \lambda^{2^j+1 p^n},$$

it may happen that λ^{2^j+1} is in the $GF[p^n]$. This can only happen when $p^n + 1$ is a power of 2, and hence only when $d = 2$. Since in that case $p^n + 1$ is always divisible by 2^k, it is necessary that $p^n + 1$ be exactly 2^k. If this condition be satisfied, the values $j = k - 1$ and $j = k$ are such that λ^{2^j+1} is in the $GF[p^n]$ (e. g. $p^n = 3$, $k = 2$; $p^n = 7$, $k = 3$). We must therefore omit the corresponding cyclic groups, otherwise they would be duplicated in the enumeration of those of type 11 (i).

In general, there will be for H, $k + 2$ sets, each containing $M/2p^n(p^{2n} - 1)^2$, conjugate cyclic subgroups, the orders being for A and B, $\frac{1}{2}(p^{2n} - 1)$; for $\{A^{2^j-1}B\}$, ($j = 1, 2, \ldots. k - 1$) it is $2^{-(j+1)}(p^{2n} - 1)$; while for $\{A^{2^k-1}B\}$ it is $2^{-k}(p^{2n} - 1)$, where 2^k is highest power of 2 contained in $\frac{1}{2}(p^{2n} - 1)$.

§24.—The period of the substitution A in G is the least integer t such that

$$\lambda^{-t(p^n+1)} = \lambda^{2t} = \lambda^{2tp^n}.$$

Hence t is a multiple of $\frac{1}{2}(p^n + 1)$, say $h\frac{1}{2}(p^n + 1)$. Then

$$\lambda^{-\frac{1}{2}h(p^n+1)^2} = \lambda^{h(p^n+1)},$$

therefore, $$h(p^n+1)[1+\tfrac{1}{2}(p^n+1)]\equiv 0, \qquad (\text{mod } p^{2n}-1),$$
or $$\tfrac{1}{2}h(p^n+3)\equiv 0, \qquad (\text{mod } p^n-1),$$
Since $[p^n+3, p^n-1]=d$, it follows that
$$\tfrac{1}{2}h=\frac{1}{d}(p^n-1), \text{ whence } t=\frac{1}{d}(p^{2n}-1),$$

except when $d=4$ and $k=2$, in which case p^n+3 is divisible by 8, so that the least value of h is $\frac{1}{4}(p^n-1)$ or $t=\frac{1}{8}(p^{2n}-1)$ (cf. §25).

Since t is even in all cases, excepting when it is $\frac{1}{8}(p^{2n}-1)$, it follows that B is of period $\dfrac{1}{d}(p^{2n}-1)$ in all cases.

The period of the substitution $A^{2^j-1}B$ considered in the group G, is the least integer t such that
$$(-\lambda)^{-2^j(p^n+1)\cdot m}=\lambda^{2^{j+1}m}=\lambda^{2^{j+1}p^n\cdot m},$$

which requires that $2^{j+1}m$ be a multiple of p^n+1, say $h(p^n+1)$. We obtain after a slight reduction, the condition
$$h\left\{\frac{p^{2n}-1}{2^{j+2}}-\frac{p^n-1}{2}-2\right\}\equiv 0, \qquad (\text{mod } p^n-1). \qquad (1)$$

Since $\frac{1}{2}(p_n-1)$ is odd when $d=2$, it follows for $j \leqq k-2$ that the least integer h satisfying this condition is $h=p^n-1$, the quantity in parenthesis being prime to p^n-1. Hence, the period t of the substitutions
$$A^{2^j-1}B \qquad (j \leqq k-2)$$
is $2^{-(j+1)}.(p^{2n}-1)$.

Where $j=k-1$, the term
$$\frac{p^{2n}-1}{2^{j+2}}=\frac{p^{2n}-1}{2^{k+1}}$$

is odd, so that the bracketed quanity in (1) is even. It results that the least value of h is now $\frac{1}{2}(p^n-1)$, and hence the period for this substitution is $2^{-(k+1)}.(p^{2n}-1)$. Finally, when $j=k$, the congruence (1) may be written
$$\tfrac{1}{2}h\left\{\frac{p^{2n}-1}{2^{k+1}}-(p^n-1)-4\right\}\equiv 0, \qquad (\text{mod } p^n-1), \qquad (2)$$

showing that $h=2(p^n-1)$ and the period t is then $2^{-k}(p^{2n}-1)$.

The result is that for $d=2$ the periods of all the substitutions remain unchanged in passing to G, with the one exception $j=k-1$. The corresponding substitution being of period one-half of the period of the substitution in G from which it is derived.

When $d=4$, the congruence (1) may be written

$$h\left\{\frac{p^{2n}-1}{2^{j+3}}-\frac{p^n-1}{4}-1\right\}\equiv 0, \qquad \left(\text{mod}\,\frac{p^n-1}{2}\right), \qquad (3)$$

The highest power of 2 contained in p^n-1 is now 2^k. Hence, when $k>2$, $\frac{p^n-1}{4}$ is even, so that the quantity in the bracket is prime to $\frac{p^n-1}{2}$, for $j \leqq k-2$. Therefore,

$$h=\tfrac{1}{2}(p^n-1), \quad t=2^{-(j+2)}.\,p^{2n}-1.$$

If $j=k-2$, the quantity in brackets is divisible by 2. Hence,

$$h=\tfrac{1}{4}(p^n-1), \quad t=2^{-(k+1)}.\,(p^{2n}-1).$$

When $j=k-1$, congruence (3) shows that

$$h=p^n-1, \quad t=2^{-k}(p^{2n}-1),$$

and when $j=k$, writing (3) in the form

$$\tfrac{1}{4}h\left\{\frac{p^{2n}-1}{2^{k+1}}-(p^n-1)-4\right\}\equiv 0, \qquad \text{mod}\,\frac{p^n-1}{2}\Big).$$

we see that $h=2(p^n-1)$ and $t=2^{-k}(p^{2n}-1)$.

The results, then, for $d=4$ are that the cyclic subgroups in G are of orders one-half the orders of the corresponding groups in H, with the exception of those for which j has the values k, $k-1$, $k-2$, the corresponding groups being of orders, the same for the first two, as in H and for the last, one-fourth of the order of the corresponding group in H.

§25.—The most general substitution of type 6 is of one of the two forms A or A^tB. The multipliers of $A^{t-1}B$ being

$$-\rho^{-t}, \quad -\rho^{-t}, \quad \lambda^{2t}, \quad \lambda^{2tp^n},$$

the multipliers of $\Theta^2A^{t-1}B$ will be the negative of these. Since

$$-\lambda^{2t}=\lambda^{\frac{p^{2n}-1}{2}+2t},$$

we see that when $d = 2$, $\Theta^2 A^{t-1} B = A^{t'}$, where

$$t' = \tfrac{1}{2}\left[\frac{p^{2n}-1}{2} + 2t\right],$$

for $$\rho^{-t'} = \rho^{-(p^n-1)\left(\frac{p^n+1}{4}\right)} . \rho^{-t} = \rho^{-t}.$$

Hence, when $d = 2$, any substitution of the type is of the form A^t or $\Theta^2 A^{t'}$. Therefore in G there will be a *single* set of

$$M \mid 2p^n (p^{2n} - 1)^2$$

conjugate cyclic subgroups of order $\frac{1}{2}(p^{2n} - 1)$.

When $d = 4$, the substitution $A^{t-1}B$ is the same as ΘA^r (the case $k = 2$ excepted), where $r = t - \frac{1}{8}(p^{2n} - 1)$. For, the multipliers of ΘA^r are

$$\theta\rho^{-r}, \quad \theta\rho^{-r}, \quad \lambda^{2t}, \quad \lambda^{2tp^n}$$

Hence, we must have $\theta\rho^{-r} = -\rho^{-t}$. Since $\theta = \rho^{\frac{p^n-1}{4}}$,

$$\theta\rho^{-r} = \theta\rho^{-t}, \quad \rho^{\frac{p^n-1}{4} \cdot \frac{p^n+1}{2}} = \theta \,.\, \rho^{-t} . \theta^{\frac{p^n+1}{2}} = \theta^2 \rho^{-t} = -\rho^{-t}$$

when l is even (i. e $k > 2$), where $p^n = 4l + 1$.

When $k = 2$, both $\{A\}$ and $\{B\}$ produce distinct cyclic subgroups in G but of order $\frac{1}{8}(p^{2n} - 1)$ (cf. §24). In all other cases there is a single set of

$$M \mid 2p^n (p^{2n} - 1)^2$$

conjugate cyclic subgroups of order $\frac{1}{4}(p^{2n} - 1)$.

In §20 it was shown that the equation

$$\alpha^2 \lambda^{p^n+1} = 1$$

could be satisfied by $p^n(p^n - 1)$ values of α and λ when $d = 1$, and by $(p^n - 1)^2$ when $d = 2$ or 4. Accounting for permutations, these solutions produce respectively $\frac{1}{2}p^n(p^n - 1)$ and $\frac{1}{2}(p^n - 1)^2$ sets of conjugate substitutions, each set containing

$$M \mid p^n (p^{2n} - 1)^2$$

distinct substitutions, making a total of

$$M \mid 2(p^n - 1)(p^n + 1)^2 \quad \text{for } d = 1,$$
$$M \mid 2p^n (p^n + 1)^2 \qquad \text{for } d = 2$$

distinct substitutions reducible to this type.

Type 6 (ii).

§26 —The general substitution S of this type is

$$x' = \alpha x, \quad y' = \alpha (y + x), \quad z' = \lambda^t z, \quad w' = \lambda^{tp^n} w, \qquad (\alpha^2 \lambda^{t(p^n+1)} = 1),$$

where λ is a primitive root of the $GF[p^{2n}]$. When $d = 1$ there will be a single set of conjugate cyclic subgroups of order $2(p^{2n} - 1)$, of which the typical generator may be taken as the substitution S with $t = 1$. It is evident that this set will contain all the substitutions of the set of type 6 (i) for $d = 1$.

There are $p^n(p^{2n} - 1)$ substitutions commutative with S, viz.

$$x' = ax, \quad y' = bx + ay, \quad z' = \lambda^r z, \quad w' = \lambda^{rp^n} w, \qquad (a^2 \lambda^{r(p^n+1)} = 1).$$

The number of substitutions conjugate to S is therefore

$$M/p^n(p^{2n} - 1)$$

But S and the $p^{2n} + p^n - 1$ power of S are conjugate since their multipliers are only permuted. Hence there are in the set

$$M | 2p^n(p^{2n} - 1)$$

conjugate cyclic subgroups when $d = 1$.

When $d = 2$ or 4, there will be an arrangement of complete sets of conjugate subgroups similar to that for type 6 (i). The two generators A and B now take the form

$$\begin{aligned} A:\ & x' = \rho^{-1} x, & y' &= \rho^{-1}(y + x), & z' &= \lambda^2 z, & w' &= \lambda^{2p^n} w, \\ B:\ & x' = -\rho^{-1} x, & y' &= -\rho^{-1}(y + x), & z' &= \lambda^2 z, & w' &= \lambda^{2p^n} w, \end{aligned}$$

where, as before, $\rho = \lambda^{p^n+1}$. The periods of A and B are both $\frac{1}{2}p(p^{2n} - 1)$, and since $AB = BA$ and $A^2 = B^2$, we may apply directly the results of §22, putting

$$m = \tfrac{1}{2}p(p^{2n} - 1).$$

The formulation of the number of sets of conjugate cyclic subgroups is the same as for 6 (i), and hence will not be repeated here. It must be noticed, however, that each generator is conjugate with $2(p - 1)$ of its powers, viz. all those that have the same multipliers and in which the exponent of the power is not divisible by p (cf. §15).

The number of ways the canonical form can be set up is the same as for type 6 (i). Hence if $d = 1$, there are $\frac{1}{2} p^n (p^n - 1)$ sets, and when $d = 2$ or 4, there are $\frac{1}{2} (p^n - 1)^2$ sets, each containing

$$M | p^n (p^{2n} - 1)$$

distinct conjugate substitutions.

§27.—When the characteristic equation has all its roots in the $GF[p^n]$, the determinant of the substitutions is $\alpha\beta\gamma\delta = 1$. For the types 7, 8, 9, 10 and 11, it is necessary to know how many solutions there are of this equation, with the assigned equality relations amongst the roots peculiar to the respective canonical forms. The question will first be taken up for $d = 1$.

Solutions of the Equations $\alpha\beta\gamma\delta = 1$ *when* $d = 1$.

The total number of possible solutions is evidently $(p^n - 1)^3$. If three of the multipliers $\alpha, \beta, \gamma, \delta$ be equal say $\alpha = \beta = \gamma \neq \delta$, then $\alpha^3\delta = 1$, which has $(p^n - 2)$ solutions $\alpha \neq \delta$. Since any three out of the four may be equal, there are in all $4(p^n - 2)$ solutions with just three multipliers equal (cf. type 9). Just two of the multipliers will be equal for six times the number of solutions of

$$\alpha^2\gamma\delta = 1, \qquad (\alpha \neq \gamma \text{ or } \delta).$$

For the $p^n - 2$ values of $\alpha \neq 0$ or 1, γ may take $p^n - 4$ values, since it cannot equal $0, \alpha, \alpha^{-1}$ or α^{-3}. If $\alpha = 1$, γ may take $p^n - 2$ values, $\neq 0$ or 1. For each pair of values of α and γ thus assigned, δ is determined and is unequal to them. Hence there are

$$6[(p^n - 2)(p^n - 4) + (p^n - 2)] = 6(p^n - 2)(p^n - 3)$$

solutions with only two multipliers equal (cf. type 8).

For each of the $p^n - 2$ values of α, $\alpha \neq 1$ or 0 and $\beta = \alpha$, there is one value of γ, viz. $\gamma = \alpha^{-1}$ such that $\delta = \gamma$. Hence, there are $3(p^n - 2)$ sets of solutions with the multipliers equal in pairs (cf. type 11).

Excluding the identity, there remain

$$(p^n - 1)^3 - 4(p^n - 2) - 6(p^n - 2)(p^n - 3) - 3(p^n - 2) - 1$$
$$= (p^n - 2)(p^n - 3)(p^n - 4)$$

sets with all the multipliers distinct (cf. type 7).

§28.—*Solutions of the Equation* $\alpha\beta\gamma\delta = 1$ *when* $d = 2$ *or* 4.

For the $p^n - d - 1$ values of α, $\alpha \neq 0$, and not equal to d of the quantities $1, \theta, \theta^2, \theta^3$ present in the field, the mark γ takes $p^n - 5$ values, satisfying the condition that $\gamma \neq \alpha$, but $\gamma = \delta$, the excluded values of γ being 0, $\pm \alpha^{-1}$, α, α^{-3}. For the d values of α, viz. $1, \theta, \theta^2, \theta^3$, γ takes $p^n - 3$ values, for in this case $\theta^3 = \theta$, $\theta^{-1} = \theta^3$ and $-\theta^{-1} = \theta$, so that only three values for γ must be excluded. Allowing for permutations, there are then

$$6(p^n - d - 1)(p^n - 5) + 6d(p^n - 3)$$

sets of solutions with only two multipliers equal.

For every value of $\alpha \neq 1, \theta, \theta^2, \theta^3$, there are two values of γ, viz. $\pm \alpha^{-1}$, for which $\alpha = \beta$ and $\gamma = \delta$, $(\alpha \neq \gamma)$; and for each of the d values $1, \theta, \theta^2, \theta^3$, there is one such solution. Hence there will be

$$6(p^n - d - 1) + 3d$$

sets of multipliers equal in pairs. There will be $4(p^n - 1 - d)$ with just three equal and d sets with all four equal. There remain, therefore,

$$(p^n - 1)^3 - 4(p^n - d - 1) - 6(p^n - d - 1)(p^n - 5)$$
$$- 6d(p^n - 3) - 6(p^n - d - 1) - 4d,$$

or
$$p^{3n} - 9p^{2n} + 29p^n - 6d - 21$$

sets with all of the multipliers distinct. (This formula does not hold for $d = 1$, as may be seen by comparing the two results.)

Type 7

§29.—Since four unequal multipliers may be permuted in 24 distinct ways, it follows from the preceding articles that there are $\frac{1}{24}g$ distinct substitutions of this type where

$$g = (p^n - 2)(p^n - 3)(p^n - 4), \qquad (d = 1),$$
$$g = p^{3n} - 9p^{2n} + 29p^n - 6d - 21, \qquad (d = 2 \text{ or } 4).$$

There are $(p^n - 1)^3$ commutative substitutions for this type, viz.

$$x' = ax, \quad y' = by, \quad z' = cz, \quad w' = ew, \qquad (abce = 1).$$

Hence, there are $\frac{1}{24}g$ sets of conjugate substitutions, each set containing $M/(p^n - 1)^3$ substitutions of period a factor of $p^n - 1$.

The number of distinct substitutions of this type of period exactly $p^n - 1$, can be shown to be

$$\tfrac{1}{24}[F_3(p^n - 1) - 6F_2(p^n - 1) + 11F_1(p^n - 1)],$$

where

$$F_i(p^n-1)=(p^n-1)^i\left(1-\frac{1}{p_1^i}\right)\left(1-\frac{1}{p_2^i}\right)\cdots\cdots\left(1-\frac{1}{p_k^i}\right),$$

$p_1 \cdots\cdots p_k$ being the distinct prime factors of p^n-1. $F_i(p^n-1)$ designates the number of ways of choosing i integers equal to or less than p^n-1, the different permutations of the i integers being considered, and such that their greatest common divisor with p^n-1 is unity.*

Type 8 (i).

§30. $$S:\quad x'=\alpha x,\quad y'=\alpha y,\quad z'=\beta z,\quad w'=\gamma w,\qquad (\alpha^2\beta\gamma=1).$$

In §§27, 28, the number of sets of multipliers, say q, for this type was shown to be

$$6(p^n-2)(p^n-3),\qquad (d=1),$$
$$6[(p^n-1)(p^n-5)+2d],\qquad (d=2 \text{ or } 4).$$

But four letters, two of which are equal, may be permuted in 12 distinct ways. Hence there are $\frac{q}{12}$ sets of conjugate substitutions.

There are $p^n(p^n-1)^3(p^n+1)$ substitutions commutative with S, viz.

$$x'=ax+by,\quad y'=a'x+b'y,\quad z'=cz,\quad w'=ew,$$
$$[ce(ab'-a'b)]=1.$$

Hence each one of the $\frac{q}{12}$ sets contains

$$M/p^n(p^n-1)^3(p^n+1)$$

conjugate substitutions of period a factor of p^n-1.

Type 8 (ii).

§31.—There are $p^n(p^n-1)^2$ substitutions commutative with a substitution of this type, viz. all of those of the form

$$x'=ax,\quad y'=bx+ay,\quad z'=cz,\quad w'=ew,\qquad (abc^2=1).$$

Hence the $\frac{q}{12}$ sets for this type each contain

$$M/p^n(p^n-1)^2$$

---

* Jordan, "Traité des Substitutions," p. 96.

conjugate substitutions each of period a factor of $p\,(p^n-1)$.

Type 9 (i).

§32.—A substitution

$$S:\quad x'=\rho x,\quad y'=\rho\,(y+x),\quad z'=\rho\,(z+y),\quad w'=\rho^{-3}w$$

exists for which ρ is a primitive root of the $GF\,[p^n]$. Since S^m is

$$x'=\rho^m x,\quad y'=\rho^m\,(y+mx),\quad z'=\rho^m\,(z+my+\tfrac{1}{2}m\,(m-1)\,z),\quad w'=\rho^{-3m}w$$

the period of S is $p\,(p^n-1)$ for $p>2$, and for $p=2$ it is $4\,(2^n-1)$.

The most general substitution W of this type has the form

$$x'=\rho^k x,\quad y'=\rho^k\,(y+x),\quad z'=\rho^k\,(z+y),\quad w'=\rho^{-3k}w$$

Hence W is the power $(k-1)(p^n-1)+k$ of S. For

$$\rho^{(k-1)(p^n-1)+k}=\rho^k$$

and $$(k-1)(p^n-1)+k\equiv 1,\qquad (\mathrm{mod}\ p).$$

Therefore there is a single set of conjugate cyclic subgroups for this type.

There are $p^{2n}\,(p^n-1)$ substitutions commutative with S, viz.

$$x'=ax,\quad y'=bx+ay,\quad z'=cx+by+az,\quad w'=ew,\qquad (a^3e=1),$$

and hence $$M/p^{2n}\,(p^n-1)$$
conjugate with it.

When $d=1$, S and S^{2p^n-1} are conjugates, and when $d=2$ or 4, S will be conjugate with all of its powers such that

$$m\equiv 1\ (\mathrm{mod}\ p^n-1),\quad m\not\equiv 0,\ (\mathrm{mod}\ p).$$

Hence m has the form $h\,(p^n-1)+1$, where h can take all the values $2, 3 \ldots\ldots p$; so S is conjugate with $(p-1)$ of its powers. Indeed, a substitution V transforming S into S^m (m not divisible by p) is

$$x'=x,\quad y'=my,\quad z'=x+\tfrac{1}{2}m\,(m-1)\,y+m^2z,\quad w'=aw,\qquad (m^3a=1).$$

Hence, when $d=1$, the set contains

$$M/2p^{2n}\,(p^n-1)$$

conjugate cyclic subgroups of order $4\,(2^n-1)$, and when $d=2$ or 4, it has

$$M/(p-1)\,p^{2n}\,(p^n-1)$$

such subgroups, each being of order $p\,(p^n-1)$.

The period of S in G for $d > 1$ is the least integer $t.p$ such that

$$\rho^t = \rho^{-3t} \quad \text{or} \quad \rho^{4t} = 1.$$

Hence $t = \frac{1}{d}(p^n - 1)$ and $pt = \frac{1}{d}p(p^n - 1)$. Therefore the set in G contains the same number of cyclic subgroups as the set in H, but of orders reduced in the ratio $1 : d$.

From the results of §§26, 27, it follows that there are in H, $p^n - d - 1$ distinct sets each containing

$$M/p^{2n}(p^n - 1)$$

conjugate substitutions, and in G there are $\frac{1}{d}(p^n - d - 1)$ such sets.

Type 9 (ii).

§33.—There will be a single set of conjugate substitutions for this type, of which the typical generator is

$$S: \quad x' = \rho x, \quad y' = \rho(y + x), \quad z' = \rho z, \quad w' = \rho^{-3} w,$$

where again ρ is a primitive root of the $GF[p^n]$. The period of S is $p(p^n - 1)$ for all cases, and the period of the corresponding substitution in G is $\frac{1}{d}p(p^n - 1)$.

There are $p^{3n}(p^n - 1)^2$ substitutions commutative with S, viz.

$$x' = ax, \quad y' = bx + ay + cz, \quad z' = ex + fz, \quad w' = gw, \qquad (a^2fg = 1),$$

and hence there are

$$M/p^{3n}(p^n - 1)^2$$

substitutions conjugate to S. But S is conjugate with $p - 1$ of its powers, viz. those whose exponents are

$$m = h(p^n - 1) + 1, \qquad (h = 2, 3, \ldots . p).$$

Indeed, the substitution

$$x' = x, \quad y' = my, \quad z' = z, \quad w' = aw \qquad (am = 1)$$

transforms S into S^m. Hence there are

$$M/(p - 1)p^{3n}(p^n - 1)^2$$

conjugate cyclic subgroups in the set.

From §§26, 27, it follows that there are in H $p^n - d - 1$ sets of conjugate substitutions for this type, each set containing

$$M/p^{3n}(p^n - 1)^2$$

substitutions, and in G there are $\frac{1}{d}(p^n - d - 1)$ such sets.

Type 9 (iii).

§34.—The typical generator in this case is

$$S: \quad x' = \rho x, \quad y' = \rho y, \quad z' = \rho z, \quad w' = \rho^{-3} w$$

of period $p^n - 1$ in H and $\frac{1}{d}(p^n - 1)$ in G.

The commutative substitution T in this case will have the form

$$x' = a_1 x + b_1 y + c_1 z, \quad y' = a_2 x + b_2 y + c_2 z, \quad z' = a_3 x + b_3 y + c_3 z, \quad w' = ew$$

with determinant

$$e \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = 1.$$

The number of ways this determinant can be set up is equal to the order of the general ternary group, viz.

$$s = (p^{3n} - 1)(p^{3n} - p^n)(p^{3n} - p^{2n}).$$

Since s is not conjugate with any of its powers, there are M/s conjugate cyclic subgroups in the set, each group containing $p^n - d - 1$ substitutions reducible to this canonical form. In G there will be the same arrangement of cyclic subgroups with the order of each $\frac{1}{d}(p^n - 1)$ instead of $p^n - 1$.

Type 10 (i).

§35.—The general substitution S of this type has the form

$$x' = ax, \quad y = \alpha(y + x), \quad z' = \alpha(z + y), \quad w' = \alpha(w + z), \qquad (\alpha^4 = 1).$$

When $d = 1$, $\alpha = 1$; $d = 2$, $\alpha = \pm 1$, and when $d = 4$, $\alpha = 1$, θ, θ^2 or θ^3, where θ denotes always a primitive root of the equation $d^4 = 1$. Hence, there are in H, d sets of conjugate substitutions. To find the period of S, consider S^m, viz.

$$x' = \alpha^m x, \quad y' = \alpha^m (y + mx), \quad z' = \alpha^m \left(z + my + \frac{m(m-1)}{2} x \right),$$
$$w' = \alpha^m \left(w + mz + \frac{m(m-1)}{2} y + \frac{m(m-1)(m-2)}{6} x \right).$$

When $d = 1$, i. e. $p = 2$ and $\alpha = 1$, the period is evidently 4; for $p = 3$ the period is 9 for $\alpha = +1$ and 18 for $\alpha = -1$. For $d = 2$, $p \neq 3$, the period is p or $2p$, according as $\alpha = +1$ or $\alpha = -1$. When $d = 4$, the period is p, $4p$, $2p$ or $4p$, according as $\alpha = 1, \theta, \theta^2$ or θ^3 respectively.

The following substitution W

$$x' = a_1 x, \quad y' = a_2 x + m a_1 y, \quad z' = a_3 x + \tfrac{1}{2}[2 m a_2 + m(m-1) a_1] y + m^2 a_1 z,$$
$$w' = a_4 x + [m a_3 + \tfrac{1}{2} m (m-1) a_2 + \tfrac{1}{6} m (m-1)(m-2) a_1] y$$
$$+ \tfrac{1}{2}[2 m^2 a_2 + m^2 (m-1) a_1 + m^2 (m-1) a_1] z + m^3 a_1 w$$

is the most general substitution transforming S into S^m. The determinant of W being $m^6 a_1^4$, is different from zero only when m is not a multiple of p, and in that case the determinant can be made equal to unity by properly choosing a_1. Hence S is conjugate with all its powers, the exponents of which are not multiples of p.

There are dp^{3n} substitutions commutative with S, viz.

$$x' = ax, \quad y' = bx + ay, \quad z' = cx + by + az, \quad w' = fx + cy + bz + az, \qquad (a^4 = 1).$$

Hence, there are M/dp^{3n} substitutions conjugate to S.

In the particular case $p = 3$, the substitutions S, S^2, S^4, S^5, S^7 and S^8 are conjugates when $\alpha = +1$, making in the set $\dfrac{M}{6dp^{3n}} = \dfrac{M}{324}$ conjugate cyclic subgroups of order 9. When $p = 3$ and $\alpha = -1$, S is conjugate with 12 of its powers, giving them a set of $\dfrac{M}{648}$ subgroups of order 18.

When $d = 2$, $p > 3$, the substitution S is conjugate with $p - 1$ of its powers when $\alpha = 1$, and with $2(p - 1)$ when $\alpha = -1$. It results, therefore, that the corresponding sets contain respectively

$$M/2(p-1)p^{3n}, \quad M/4(p-1)p^{3n}$$

conjugate cyclic subgroups with orders p and $2p$.

When $d = 4$, S is conjugate with $p-1$, $2(p-1)$ or $4(p-1)$ of its powers according as α is $+1$, -1 or θ or θ^3. The four sets have, then, respectively,

$$M/4(p-1)p^{3n}, \quad M/8(p-1)p^{3n}, \quad M/16(p-1)p^{3n}$$

conjugate cyclic subgroups.

Since in each of the d sets of conjugate substitutions, there are M/dp^{3n} substitutions, the total number of substitutions reducible to this canonical form is M/p^{3n}.

§36.—The period of S in the fractional group G is independent of α, and is equal to 4 when $d = 1$; for $d = 2$ and $p = 3$, it is 9; for $d = 2$, $p \neq 3$, and for $d = 4$, it is p. In all cases there is a single set of conjugate cyclic subgroups. The number of substitutions conjugate to S in G is M/p^{3n}, the same as in H. For $d = 1$, the structure of the set is, of course, the same in both groups, and generally the set in G is abstractly identical with the corresponding set in H arising for $\alpha = 1$. In passing to G, the d sets of H are absorbed into this one.

By a discussion analogous to that of §16, the d subtypes 10 (i), 10′ (i), 10″ (i) and 10‴ (i) that are present may each be shown to have a structure identical with that of 10 (i) just discussed. Hence, the group G has d sets of conjugate cyclic subgroups arising from this type.

Type 10 (ii).

§37.—There are d sets of conjugate cyclic subgroups for this type of which the general substitution S is

$$x' = \alpha x, \quad y' = \alpha(y + x), \quad z' = \alpha(z + y), \quad w' = \alpha w, \qquad (\alpha^4 = 1).$$

The period of S is 4 when $p = 2$ (i. e. $d = 1$ and $\alpha = 1$); for $\alpha = 1$, $p \neq 2$, the period is p; for $\alpha = -1$, it is $2p$, and for $\alpha = \theta$ or θ^3, it is $4p$ (cf. §35).

If m is prime to p, the substitution

$$x' = x, \quad y' = m^{-1}y, \quad z' = z - \frac{m-1}{2m}y, \quad w' = mw$$

transforms S into S^m. Hence, for $p = 2$, S and S^3 are conjugates. If $\alpha = 1$, $p \neq 2$, S is conjugate with $p-1$ of its powers, if $\alpha = -1$, with $2(p-1)$ powers, and if $\alpha = \theta$ or θ^3, with $4(p-1)$ of its powers. Since there are

$p^{4n}(p^n-1)$ substitutions

$$x' = a_1x,\ y' = a_2x + a_1y,\ z' = a_3x + a_2y + a_1z + a_4w,\ w' = a_5x + a_6w,\quad (a^3f = 1),$$

it follows that the set for $p = 2$, $(d = 1)$ contains

$$M/2p^{4n}(p^n-1)$$

subgroups; when $\alpha = 1$, $p \neq 2$, the set contains

$$M/(p-1)p^{4n}(p^n-1)$$

subgroups; when $\alpha = -1$, there are

$$M/2(p-1)p^{4n}(p^n-1);$$

and when $\alpha = \theta$ or θ^3, there will be

$$M/4(p-1)p^{4n}(p^n-1)$$

subgroups in the set.

Since there are $M/p^{4n}(p^n-1)$ substitutions in each of the d complete sets of conjugate substitutions, it follows that there are in H

$$dM/p^{4n}(p^n-1)$$

substitutions reducible to this canonical form.

The structure of the set in G is again the same as the set in H given by $\alpha = 1$ (cf. §36), the d sets of the group H being merged into a single set in G.

Type 10 (iii).

§38.—As in the two preceding cases, there are d types corresponding to the d solutions of $\alpha^4 = 1$, viz.

$$S:\quad x' = \alpha x,\quad y' = \alpha(y + x),\quad z' = \alpha z,\quad w' = \alpha w,\qquad (\alpha^4 = 1).$$

If $\alpha = 1$, the period is equal to p for all cases. The periods for the other values of α are the same as in type 10 (ii), and here also S will be conjugate with all its powers, the exponents of which are prime to p.

There are $$s \equiv p^{5n}(p^{2n}-1)(p^{2n}-p^n)$$

substitutions commutative with S, viz.

$$x' = a_1x,\quad y' = a_2x + a_1y + a_3z + a_4w,$$
$$z' = a_5x + a_6z + a_7w,\quad w = a_8x + a_9y + a_{10}w,\qquad (a_1^2\Delta = 1),$$

where $\Delta = (a_6 a_{10} - a_7 a_9)$. For each of the $p^n - 1$ values of $a_1 \neq 0$, Δ is determined, so that there are $(p^{2n} - 1)(p^{2n} - p^n)$ corresponding sets of values for a_6, a_{10}, a_7, a_9. Hence there are s solutions of $a_1^2 \Delta = 1$.

When $\alpha = 1$, therefore, there are

$$M/s\,(p-1)$$

conjugate cyclic subgroups in the set; when $\alpha = -1$, or $\alpha = \theta$ or θ^3, there are respectively

$$M/2s\,(p-1) \quad \text{and} \quad M/4s\,(p-1)$$

such subgroups. The results for G will again be gotten by putting $\alpha = 1$, giving in all cases one set of conjugate cyclic subgroups.

Type 10 (iv).

§39.—There are d sets for this type, of which the general substitution is

$$S\colon\quad x' = \alpha x, \quad y' = \alpha(y + x), \quad z' = \alpha z, \quad w' = \alpha(w + z),$$

the period of S being in all cases exactly as in the preceding type, and S being conjugate with all its powers, the exponents of which are not divisible by p.

The most general substitution T commutative with S has the canonical form

$$x' = a_1 x + a_2 z, \quad y' = a_3 x + a_1 y + a_4 z + a_2 w,$$
$$z' = a_6 x + a_7 z. \quad w' = a_8 x + a_6 y + a_{10} z + a_7 w$$

with determinant

$$\Delta \equiv \begin{vmatrix} a_1 & 0 & a_2 & 0 \\ a_3 & a_1 & a_4 & a_2 \\ a_6 & 0 & a_7 & 0 \\ a_8 & a_6 & a_{10} & a_7 \end{vmatrix} \equiv \begin{vmatrix} a_1 & a_2 & 0 & 0 \\ a_6 & a_7 & 0 & 0 \\ a_3 & a_4 & a_1 & a_2 \\ a_8 & a_{10} & a_6 & a_7 \end{vmatrix} \equiv (a_1 a_7 - a_2 a_6)^2 = 1$$

Hence when $d = 1$, there are

$$s = p^{5n}(p^{2n} - 1)$$

substitutions commutative with S, and when $d = 2$ or 4 there are 2 such substitutions, and consequently M/s and $M/2s$ substitutions conjugate with S respectively. Therefore, when $d = 1$ the set contains M/s subgroups, when $\alpha = 1$, $d \neq 1$, it contains $M/2s\,(p-1)$ subgroups; when $\alpha = -1$, it has $M/4\,(p-1)\,s$, and when $\alpha = \theta$ or θ^3, there will be $M/8\,(p-1)\,s$ conjugate cyclic subgroups.

Since the structure of type $10'$ (iv) is exactly the same as for this type, each of the above results are duplicated for that type when $d = 2$ or 4.

The group G contains a single set of conjugate cyclic subgroups from type 10 (iv) abstractly identical with the set in H given by $\alpha = 1$. When $d = 2$ or 4, $10'$ (iv) also produces a set in G distinct from the preceding one.

Altogether, types 10 (iv) and $10'$ (iv) give rise to dM/s substitutions in H and to M/s substitutions in G.

Type 10 (v).

§40.—The substitution

$$x' = \alpha x, \quad y' = \alpha y, \quad z' = \alpha z, \quad w' = \alpha w, \qquad (\alpha^4 = 1)$$

is one of the substitutions Θ^i, α taking d of the values $1, \theta, \theta^2, \theta^3$. These d substitutions form precisely the invariant subgroup that defines the isomorphism between H and G.

Type 11 (i).

§41.—The general substitution of this type has the canonical form

$$S: \quad x' = \alpha x, \quad y' = \alpha y, \quad z' = \beta z, \quad w' = \beta w, \qquad (\alpha^2\beta^2 = 1, \ \alpha \neq \beta)$$

the period of which is $p^n - 1$. If ρ is a primitive root of the $GF[p^n]$, then when $d = 1$, every substitution of the above form is a power of the substitution with multipliers $\rho, \rho, \rho^{-1}, \rho^{-1}$. There will be in H and in G, therefore, a single set of conjugate cyclic subgroups.

The most general substitution commutative with one of this type is

$$x' = a_1 x + b_1 y. \quad y' = a_2 x + b_2 y, \quad z' = c_1 z + d_1 w, \quad w' = c_2 z + d_2 w,$$

with determinant

$$(a_1 b_2 - a_2 b_1)(c_1 d_2 - c_2 d_1) = 1.$$

One of the factors may be chosen arbitrarily in $(p^{2n} - 1)(p^{2n} - p^n)$ ways; the other factor, being then determined by the above relation, can be satisfied in $p^n (p^{2n} - 1)$ ways. Hence in all there are

$$s = (p^{2n} - p^n)^2 (p^n + 1)^2 (p^n - 1)$$

commutative substitutions. Since the only power of S conjugate to S is S^{-1}, there will be in H and in G for $d = 1$, $M/2s$ conjugate cyclic subgroups in the set, each subgroup containing $p^n - 2$ substitutions reducible to this type, (cf. §27).

Type 11 (i) *for* $d = 2$ *or* 4.

§42.—In this case there will not be a single set of conjugate cyclic subgroups in H. Let A be the substitution

$$A: \quad x' = \rho x, \quad y' = \rho y, \quad z' = \rho^{-1} z, \quad w' = \rho^{-1} w,$$

and let B be the substitution

$$B: \quad x' = \rho x, \quad y' = \rho y, \quad z' = -\rho^{-1} z, \quad w' = -\rho^{-1} w.$$

Any substitution in this canonical form is then representable either in the form A^t or $A^t B$. This can be verified by noticing that the multipliers of the general substitution are

$$\rho^h, \rho^h \pm \rho^{-h}, \pm \rho^{-h},$$

which, with the plus sign, are the multipliers of A^h and with the minus sign are those of $A^{h-1}B$. Furthermore, A and B are of period $p^n - 1$ and fulfil the relations

$$AB = BA, \quad A^2 = B^2,$$

We may therefore apply directly the results of §22 to determine the cyclic subgroups.

Putting then the m of §20 equal to $p^n - 1$, k becomes the highest power of 2 contained in $p^n - 1$, so that $k = 1$ if $d = 2$, and there are in that case three cyclic subgroups

$$\{A\}, \quad \{B\}, \quad \{AB\},$$

each of order $p^n - 1$. When $d = 4$, $k \overline{\gtrless} 2$, and there are $k + 2$ cyclic subgroups, $\{A\}$ and $\{B\}$ of order $(p^n - 1)$ and

$$\{A^{2^j - 1}B\}, \qquad (j = 1, 2, \ldots . k - 1)$$

of order $2^{-j}(p^n - 1)$ respectively, and, finally, $\{A^{2^k - 1}B\}$ of order $2^{-(k+1)}(p^n - 1)$.

The substitution A is conjugate with its reciprocal. Consider the substitution $A^{2^j - 1}B$. Its multipliers are

$$\rho^{2^j}, \quad \rho^{2^j}, \quad -\rho^{-2^j}, \quad -\rho^{-2^j}.$$

The t^{th} power of this substitution will have the same set of multipliers for $t < p^n - 1$, only if

$$t \cdot 2^j \equiv \tfrac{1}{2}(p^n - 1) - 2^j, \qquad (\text{mod } p^n - 1),$$

which may be written, when $j < k$, in the form

$$(1) \quad t \equiv 2^{-(j+1)} \cdot (p^n - 1) - 1, \qquad (\text{mod } 2^{-j}(p^n - 1)).$$

Therefore we may take

$$t = 2^{-(j+1)}(p^n - 1) - 1 + h 2^{-j}(p^n - 1),$$

or

$$t = (2h + 1) 2^{-(j+1)}(p^n - 1) - 1,$$

where h may take the values $0, 1, \ldots\ 2^j - 1$. Hence, the substitution $A^{2^j-1}B$ is conjugate with 2^j of its powers. The particular value $j = 0$ gives the substitution B, which is therefore conjugate with one of its powers, viz. the power $\frac{1}{2}(p^n - 3)$.

When $j = k$, the congruence (1) has no solutions. It results, then, that the set of which $\{A\}$ is the typical subgroup, contains $M/2s$ conjugate cyclic subgroups. The set corresponding to the groups

$$\{A^{2^j-1}B\}, \qquad (j = 0, 1 \ldots\ k-1)$$

will contain $M/2^js$ such subgroups, while the set, of which $\{A^{2^k-1}B\}$ is the typical generator, will contain M/s subgroups.

§43.—The period of the substitution A considered in the group G is the least integer r such that

$$\rho^r = \rho^{-r},$$

hence for $d = 2$ or 4, r is $\frac{1}{2}(p^n - 1)$.

The period of the substitution $\{A^{2^j-1}B\}$ is the least integer r such that

$$\rho^{2^jr} = \rho^{[\frac{1}{2}(p^n-1)-2^j]r}.$$

Hence,

$$r(2^{j+1} - \tfrac{1}{2}(p^n - 1)) \equiv 0, \qquad (\text{mod.}\ p^n - 1).$$

or

$$r\left(1 - \frac{p^n - 1}{2^{j+2}}\right) \equiv 0, \qquad \left(\text{mod}\ \frac{p^n - 1}{2^{j+1}}\right),$$

Hence, for $j \overline{\gtrless} k - 3$, $r = 2^{-(j+1)}.(p^n - 1)$. When $j = k - 2$, we may write the congruence in the form

$$\tfrac{1}{2}r\left(1 - \frac{p^n - 1}{2^k}\right) \equiv 0, \qquad \left(\text{mod}\ \frac{p^n - 1}{2^k}\right),$$

so that $r = 2^{-k}.(p^n - 1)$. When $j = k - 1$, we have

$$r\left(2 - \frac{p^n - 1}{2^k}\right) \equiv 0, \qquad \left(\text{mod}\ \frac{p^n - 1}{2^{k-1}}\right),$$

hence, $r = 2^{-(k-1)}.(p^n - 1)$; finally, when $j = k$, we find $r = 2^{-(k-1)}.(p^n - 1)$.

When $d = 2$, the order of $\{A\}$ reduces one-half, while those of $\{B\}$ and $\{AB\}$ remain unchanged in passing to G. When $d = 4$, the orders of the groups

$$\{A\}, \quad \{A^{2^j-1}B\}, \qquad (j = 0, 1, 2, \ldots\ k - 3)$$

are reduced one-half; the order of the group $\{A^{2^{k-2}-1}B\}$ is reduced one-fourth, while for $j = k - 1$ and $j = k - 2$ the orders of the corresponding groups remain unchanged.

Since A has the multipliers $\rho, \rho, \rho^{-1}, \rho^{-1}$, $\Theta^2 A$ will have the negative of these as multipliers, and since

$$-\rho = \rho^{\frac{1}{2}(p^n+1)}, \quad -\rho^{-1} = \rho^{\frac{1}{2}(p^n-3)},$$

we see that $\Theta^2 A$ is A to the power $\frac{1}{2}(p^n-1)$.

The substitution $\Theta^2 B$ is not equal to any power of B but is conjugate with B^{-1}. Hence in G there are half as many cyclic subgroups in the set of which $\{B\}$ is the typical subgroup; the orders as we have seen remaining unchanged. The set of which $\{A\}$ is the typical subgroup has the orders of the subgroups shortened one-half, while the number of subgroups is unchanged.

The substitution $\Theta^2 AB$ is conjugate with $(AB)^{-1}$. Hence its properties in (G) are the same as those for the substitution B.

It will be shown that when $d=4$, all these sets of cyclic groups unite to form a single set in the group G. To this end consider $\Theta A^{2^j-1}B$ whose multipliers are

$$\theta\rho^{2^j}, \quad \theta\rho^{2^j}, \quad \theta^3\rho^{-2^j}, \quad \theta^3\rho^{-2^j},$$

where $\theta = \rho^{\frac{1}{4}(p^n-1)}$. It results that

$$\Theta A^{2^j-1}B = A^t,$$

where $t = \frac{1}{4}(p^n-1) + 2^j$. This may be verified by noticing that

$$\theta\rho^{2^j} = \rho^t \quad \text{and} \quad \theta^3\rho^{-2^j} = (\theta\rho^{2^j})^{-1} = \rho^{-t}.$$

It results that all of the substitutions of the type in H are for $d=4$ of the form A^r or ΘA^r, hence in G there is a single set of conjugate cyclic subgroups.

From §28 it follows that there are for $d=2$ or 4, $p^n-1-\frac{1}{2}d$ distinct ways of setting up this canonical form for the sets of solutions there determined, are permuted in six different ways. Hence there will be $p^n-1-\frac{1}{2}d$ complete sets of conjugate substitutions for this type, each set containing M/s distinct substitutions.

In the group G there will be, for $d=2$, $\frac{1}{2}(p^n-1)$ sets of conjugate substitutions; for among the p^n-2 sets in H, will occur the multipliers $(1, 1, -1, -1)$ which are simply permuted if one multiplies by θ^2, while the other sets of multipliers are permuted in pairs. When $d=4$, there is also the set $(\theta, \theta, \theta^3, \theta^3)$ which unites with the set $(-1, -1, 1, 1)$ to form a single substitution in G. The remaining p^n-5 substitutions in H unite by fours; hence in all there are $\frac{1}{4}(p^n-1)$ distinct sets. In general, then, there are, for $d=2$ or 4, $\frac{1}{d}(p^n-1)$ sets of conjugate substitutions, all but one containing M/s substitutions. The exceptional set is the one arising from the multipliers $(-1, -1, 1, 1)$ when $d = 2$, and the one coming from the sets of multipliers $(-1, -1, 1, 1)$ and $(\theta, \theta, \theta^3, \theta^3)$ when $d = 4$. This set comes under the discussion of §11, the multipliers in the homogeneous group being of the form

$$M_1, \frac{1}{M_1}, \theta^2 M_1, \frac{\theta^2}{M_1},$$

Hence, there are one-half as many conjugate substitutions in G as in H, so that this set contains $M/2s$ conjugate substitutions.

Type 11 (ii).

§44.—The general substitution of this canonical form is

$$S: \quad x' = \alpha x, \quad y' = \alpha(y+x), \quad z' = \beta z, \quad w' = \beta(w+z). \qquad (\alpha^2\beta^2 = 1),$$

the period of which in H is $p(p^n - 1)$ or a factor of it, while the period of S in G is $\frac{1}{2}p(p^n - 1)$.

When $d = 1$, there are $p^{2n}(p^n - 1)$ substitutions T commutative with S, and when $d = 2$ or 4, there are $2p^{2n}(p^n - 1)$ such substitutions, viz. all of the form

$$x' = a_1 x, \quad y' = a_2 x + a_1 y, \quad z' = b_1 z, \quad w' = b_2 z + b_1 w, \qquad (a_1^2 b_1^2 = 1).$$

Just as for type 11 (i) there will be a single set of conjugate substitutions and since S and S^{2p^n-3} are the only powers of S that are conjugate, there will be $M/2p^{2n}(p^n - 1)$ substitutions in the set.

When $d = 2$ or 4, there will be an arrangement of sets of conjugate cyclic subgroups corresponding to that for the preceding type. In determining the number of cyclic subgroups in the set in H, it must be noticed that the generator is conjugate with all its powers, the exponents of which are prime to p and which have the same set of multipliers.

There will be in H, $p^n - 1 - \frac{1}{2}d$ sets of conjugate substitutions, each set containing

$$M/2p^{2n}(p^n - 1)$$

substitutions.

Type 11 (iii).

§45. $\quad S: \quad x' = \rho x, \quad y' = \rho y, \quad z' = \rho^{-1} z, \quad w' = \rho^{-1}(w + z).$

The discussion of this type is similar to that for the preceding types. The period of S in H is $p(p^n - 1)$ and in G it is $\frac{1}{2}p(p^n - 1)$.

There are

$$S = p^n(p^{2n} - 1)(p^{2n} - p^n)$$

substitutions commutative with S, viz.

$$x' = a_1x + b_1y,\quad y' = a_2x + b_2y,\quad z' = a_3z,\quad w' = b_3z + a_3w,\qquad (a_3[a_1b_2 - a_2b_1] = 1).$$

In this case S is not conjugate with any of its powers for $d = 1$. Hence, the set contains M/s conjugate cyclic subgroups. Applying the results of §22, we see that as in type 11 (i) there are 3 sets of conjugate cyclic subgroups when $d = 2$, and $k + 3$ when $d = 4$, k being the highest power of 2 contained in $p^n - 1$.

When $d = 1$, there are $p^n - 2$ complete sets of conjugate substitutions, and when $d = 2$ or 4, $p^n - 1 - \frac{d}{2}$ sets, each set containing M/s substitutions.

§46.—As a partial verification of the correctness of the results, it will be found that the sum of the totals of the number of substitutions reducible to the various canonical forms in H is equal to M the order of H.

The following table shows the results for $p^n = 2$. The group is then of order 20160, and is simply isomorphic with the alternating group on 8 letters, On account of the low value of p^n, no substitutions occur for the types omitted from the table, and for each type present there is a single set of conjugate subgroups.

Type.	Order of Subgroups.	Number of Subgroups in set.	Number of Substitutions Reducible to Type.	Type of Corresponding Literal Substitutions.
1	15	336	4032	(12345) (12345)(678)
2	7	960	5760	(1234567)
4 (i)	6	840	1680	(12)(34)(567)
4 (ii)	3	56	112	(123)
6 (i)	3	560	1120	(123)(456)
6 (ii)	6	1680	3360	(123456)(78)
10 (i)	4	1260	2520	(1234)(56)
10 (ii)	4	630	1260	(1234)(5678)
10 (iii)	2	105	105	(12)(34)(56)(78)
10 (iv)	2	210	210	(12)(34)
Identity			1	
			20160	

UNIVERSITY OF CHICAGO, *May* 1, 1901.